



Calhoun: The NPS Institutional Archive
DSpace Repository

NPS Scholarship

Theses

2003-03

Computer wireless networks : a design plan
for building wireless networks using IEEE
802.11 standard

Almantheri, Hamed

Monterey, California. Naval Postgraduate School

<https://hdl.handle.net/10945/1151>

Copyright is reserved by the copyright owner.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>

NAVAL POSTGRADUATE SCHOOL

Monterey, California



THESIS

**COMPUTER WIRELESS NETWORKS: A DESIGN PLAN FOR
BUILDING WIRELESS NETWORKS USING IEEE 802.11
STANDARD**

by

Hamed Almantheri

March 2003

Thesis Advisor:
Second Reader:

Bert Lundy
Richard Riehle

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE March 2003	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Computer Wireless Networks: A Design Plan For Building Wireless Networks Using IEEE 802.11 Standard			5. FUNDING NUMBERS
6. AUTHOR(S) Hamed Almantheri			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE
13. ABSTRACT (maximum 200 words) <p>In spite of the fact that wireless network technology has been available for a long time, there has been very limited deployment of wireless networks worldwide before 1997 due to the lack of a widely recognized standard for wireless networks. Thanks to the approval of the IEEE 802.11 family of standards in 1997, the world has witnessed tremendous deployment and proliferation of wireless networks in all aspects of life.</p> <p>Although the IEEE 802.11 family of standards has been ratified to design radio transceivers for wireless computer stations capable of interconnecting with other wireless computer stations in close proximity, the technology has been successfully employed to design and implement wireless networks with a large of distant wireless computer stations with reasonable data throughput and flexibility.</p> <p>This thesis explores the wireless network technology and the primary building blocks and components of a wireless network. It also explores the IEEE 802.11 standard and its technical specifications including the Physical layer (PHY), the Media Access Control layer (MAC) and the ongoing task forces. Additionally, the thesis examines the wireless network security including the vulnerabilities, ongoing improvements and recommendations. Next, it investigates the market for available wireless devices compatible with the IEEE 802.11 standard that can be used to build a wireless network with high data throughput and a high level of security.</p> <p>Subsequently, the thesis formulates a design plan for a civilian wireless network with different scenarios in order to provide a speedy solution to the limited broadband service availability in the Sultanate of Oman. Additionally, the thesis formulates a generic design plan for a military wireless network with different scenarios that can be rapidly deployed in the field of operations.</p>			
14. SUBJECT TERMS IEEE 802.11, Media Access Control Layer, Physical Layer, Wireless Local Area Network, Wireless Point of Presence, Hotspots, WPOP, Hotspots, Access Point, Wireless Network Interface Card, Wireless Router			15. NUMBER OF PAGES 101
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**COMPUTER WIRELESS NETWORKS: A DESIGN PLAN FOR BUILDING
WIRELESS NETWORKS USING IEEE 802.11 STANDARD**

Hamed Almantheri
Computer Engineer, Royal Army of Oman
B.S., Embry-Riddle Aeronautical University, Florida 1986

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

**NAVAL POSTGRADUATE SCHOOL
March 2003**

Author: Hamed Almantheri

Approved by: Bert Lundy
Thesis Advisor

Richard Riehle
Second Reader

Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In spite of the fact that wireless network technology has been available for a long time, there has been very limited deployment of wireless networks worldwide before 1997 due to the lack of a widely recognized standard for wireless networks. Thanks to the approval of the IEEE 802.11 family of standards in 1997, the world has witnessed tremendous deployment and proliferation of wireless networks in all aspects of life.

Although the IEEE 802.11 family of standards has been ratified to design radio transceivers for wireless computer stations capable of interconnecting with other wireless computer stations in close proximity, the technology has been successfully employed to design and implement wireless networks with a large of distant wireless computer stations with reasonable data throughput and flexibility.

This thesis explores the wireless network technology and the primary building blocks and components of a wireless network. It also explores the IEEE 802.11 standard and its technical specifications including the Physical layer (PHY), the Media Access Control layer (MAC) and the ongoing task forces. Additionally, the thesis examines the wireless network security including the vulnerabilities, ongoing improvements and recommendations. Next, it investigates the market for available wireless devices compatible with the IEEE 802.11 standard that can be used to build a wireless network with high data throughput and a high level of security.

Subsequently, the thesis formulates a design plan for a civilian wireless network with different scenarios in order to provide a speedy solution to the limited broadband service availability in the Sultanate of Oman. Additionally, the thesis formulates a generic design plan for a military wireless network with different scenarios that can be rapidly deployed in the field of operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND	1
B.	OMAN’S TELECOMMUNICATION INFRASTRUCTURE	2
C.	OBJECTIVES OF THE THESIS.....	4
D.	METHODOLOGY OF THE THESIS.....	4
E.	THESIS ORGANIZATION.....	5
II.	WIRELESS NETWORKS TECHNOLOGY OVERVIEW	7
A.	INTRODUCTION.....	7
B.	WIRELESS NETWORK OVERVIEW	7
1.	Definitions.....	7
2.	History.....	7
3.	Topologies	8
4.	Protocols.....	10
5.	How Wireless Networks Work	11
6.	Types	11
a.	<i>Wireless Personal Area Network (WPAN).....</i>	<i>11</i>
b.	<i>Wireless Local Area Networks (WLANs).....</i>	<i>12</i>
c.	<i>Wide Wireless Area Networks (WWANs).....</i>	<i>13</i>
d.	<i>Wireless Metropolitan Area Networks (WMANs)</i>	<i>13</i>
7.	Basic Components and Operations of WLANs	16
C.	WHY DO WE USE WIRELESS NETWORKS?.....	20
D.	WIRELESS NETWORKS CONSIDERATIONS.....	20
1.	Physical Location and Weather Considerations	21
2.	Signal Interference Considerations	21
3.	Range, Coverage and Data Rate.....	21
4.	Compatibility and Interoperability	22
5.	Licensing Issues.....	22
6.	Security Considerations.....	22
7.	Health Issues.....	23
E.	SUMMARY	23
III.	OVERVIEW OF IEEE 802.11 STANDARD.....	25
A.	INTRODUCTION.....	25
B.	HISTORY	25
C.	IEEE 802.11 ARCHITECTURE AND SERVICES.....	26
D.	IEEE 802.11 PHYSICAL LAYER (PHY)	27
1.	Direct Sequence Spread Spectrum Physical Layer (DSSS)	29
2.	Frequency Hopping Spread Spectrum (FHSS).....	29
3.	IEEE 802.11a.....	31
a.	<i>PLCP DATA Scrambler.....</i>	<i>31</i>
b.	<i>OFDM Modulation</i>	<i>31</i>

	c.	<i>IEEE 802.11a Operating Channel Frequencies Range</i>	32
4.		IEEE 802.11b.....	33
	a.	<i>IEEE 802.11b Operating Channel Frequency Range</i>	33
	b.	<i>IEEE 802.11b Modulation and Channel Data Rates</i>	34
E.		IEEE 802.11 MEDIA ACCESS CONTROL LAYER (MAC).....	34
	1.	Basic Access Method (CSMA/CA)	35
	2.	MAC Frames.....	35
	a.	<i>Control Frames</i>	36
	b.	<i>Management Frames</i>	36
	c.	<i>Data Frames</i>	38
F.		IEEE 802.11 DRAFT STANDARDS.....	38
	1.	IEEE 802.11g.....	39
	2.	IEEE 802.11e (Quality of Service).....	39
	3.	Other IEEE 802.11 Draft Standards.....	39
G.		SUMMARY	40
IV.		WIRELESS NETWORK SECURITY.....	41
	A.	INTRODUCTION.....	41
	B.	PROBLEMS WITH WIRELESS NETWORKS SECURITY.....	42
	1.	Easy Access.....	42
	2.	Rogue Access Points.....	42
	3.	Unauthorized Use of Service.....	43
	4.	Service and Performance Limitations.....	43
	5.	MAC Spoofing and Session Hijacking.....	43
	C.	WIRED EQUIVALENT PRIVACY (WEP)	44
	1.	WEP Architecture.....	44
	2.	Attacks on the WEP.....	45
	a.	<i>Passive Attack to Decrypt Traffic</i>	45
	b.	<i>Active Attack to Insert Traffic</i>	46
	c.	<i>Active Attack from Both Ends</i>	46
	d.	<i>Table-Based Attack (Dictionary Attack)</i>	46
	3.	Software Tools to Break the WEP.....	46
	4.	Ethereal (Fingerprints Analyzer).....	47
	5.	Using Ethereal to Discover Netstumbler.....	47
	D.	IMPROVING THE IEEE 802.11 NETWORK SECURITY	48
	1.	WEP2	49
	2.	IEEE 802.1x (Port-Based Network Access Control).....	49
	a.	<i>802.1x Authentication</i>	50
	b.	<i>802.1x and Dynamic Key Management</i>	51
	c.	<i>Problems with IEEE 802.1x</i>	51
	3.	Internet Protocol Security (IPSec)	52
	E.	WIRELESS NETWORK SECURITY RECOMMENDATIONS.....	52
	F.	SUMMARY	53
V.		MARKET RESEARCH AND PRELIMINARY DESIGN	55
	A.	INTRODUCTION.....	55
	B.	MARKET RESEARCH	55

1.	Access Point	57
2.	Wireless Network Interface Cards (WNICs)	58
3.	Wireless Router (WR)	59
4.	Antennas	61
C.	DESIGN PRINCIPLES.....	63
1.	Design Plan for Oman Wireless Network.....	64
2.	Military Wireless Network.....	68
3.	A Broad Costing Plan	71
D.	SUMMARY	72
VI.	CONCLUSIONS	73
A.	SUMMARY	73
B.	CURRENT TRENDS.....	74
C.	FUTURE WORK.....	74
	LIST OF REFERENCES.....	77
	BIBLIOGRAPHY.....	81
	INITIAL DISTRIBUTION LIST	83

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Map of the Sultanate of Oman.....	4
Figure 2.	Ad-Hoc Wireless Local Area Network.....	9
Figure 3.	Infrastructure Wireless Network.....	10
Figure 4.	Wireless Personal Area Network (WPAN) [From: 5].....	12
Figure 5.	Wide Wireless Area Networks, [From: 7].....	13
Figure 6.	Wireless Metropolitan Area Networks, [From: 5].....	15
Figure 7.	Network Types, [After: 13].....	16
Figure 8.	An Access Point (AP), [From: 15].....	17
Figure 9.	Desktop Wireless PCI Adapter, [From: 16].....	18
Figure 10.	Notebook Wireless PCMCIA Adapter, [From: 16].....	18
Figure 11.	Some of the Antennas Used For Wireless Networks, [From: 18].	19
Figure 12.	Amplifier.....	19
Figure 13.	MAC And Physical Layers Location.....	28
Figure 14.	PLCP Frame Format [From: 24].....	29
Figure 15.	FHSS PLCP Frame Format.....	31
Figure 16.	MAC General Frame Format [From: 23].....	36
Figure 17.	Data Frame Format [From: 24].....	38
Figure 18.	802.1x Authentication Process, [From: 30].	50
Figure 19.	IEEE 802.1x Using Dynamic Session Keys [From: 30].....	51
Figure 20.	D-Link <i>AirPro</i> DWL-6000AP Access Point [From: 32].	57
Figure 21.	DWL-AB520 And DWL-AB650 [From: 32].	59
Figure 22.	DI-764 Wireless Router [From: 32].....	60
Figure 23.	Telex 5830AN [From: 19].	61
Figure 24.	Telex 5816AB [From: 19].	62
Figure 25.	WPOP Representation.	65
Figure 26.	Different Wireless Network Scenarios.	66
Figure 27.	Wireless Public Access Points [After: 34].....	67
Figure 28.	Muscat Wireless Network.....	67
Figure 29.	Military Wireless Network in the Field.	70

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	5 GHz Operating Channels [From: 23].....	32
Table 2.	IEEE 802.11b Data Rate Specifications [From: 23].....	33
Table 3.	High Rate PHY Frequency Channel Plan [From: 24].	34
Table 4.	Data Frame Address Field Contents [From: 24].....	38
Table 5.	NetStumbler Fingerprints.....	48
Table 6.	DWL-6000AP AP Technical Specifications [From: 32].....	58
Table 7.	DWL-AB520 And DWL-AB650 Data Sheet [From: 32].	59
Table 8.	D-Link AirPro DI-764 Wireless Router Data Sheet [From: 32].....	61
Table 9.	Telex 5830AN Electrical and Mechanical Specifications [From: 19].....	62
Table 10.	Telex 5816AB Electrical and Mechanical Specifications [From: 19].....	63
Table 11.	Approximate Cost of Basic Wireless Network Devices.....	71

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I will be forever indebted to my government and I would like to record my appreciation to the Ministry of Defense and Royal Army of Oman for providing me the opportunity for the second time in my life to achieve an advanced degree in the United States of America.

Next, I would like to thank the Naval Postgraduate School staff and faculty for the high quality of education and facilities provided during my study, and specifically, Professor Gilbert Lundy for his respect, support and directives throughout the thesis research. I would also like to register my admiration for his unique interactive lectures in the classes that made hard issues easier to comprehend. Additionally, special thanks to Professor Richard Riehle for his help and support throughout my study, and I also appreciate his respect and interest in other civilizations and cultures of the world, especially ours.

Finally, I would like to thank my friend Steve Autman for the guidelines and support throughout the years and I hope for our friendship to last forever.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

This chapter starts with a brief background on wireless network technology. Next, it provides a brief description of the telecommunications infrastructure in the Sultanate of Oman, and states the objectives of the thesis followed by description of the methodology to be used in order to accomplish the objectives. Finally, the remaining chapters are introduced.

A. BACKGROUND

Although *Wireless Local Area Network* (WLAN) technology has been available since the late 1980's, the market remained limited until the end of 1990's due to the absence of standards capable of formulating unified technical specifications and interoperability requirements for devices from different manufacturers. Thanks to the approval of the *Institute of Electrical and Electronics Engineers* (IEEE) 802.11 WLAN standard in 1997, which was further ratified in 1999, users today can join and access WLANs services without physically having to plug their workstations into the network with restraining wires. The clients can also log off and unplug their workstations without having to unplug physical cables from the network. This new type of joining and accessing computer networks has freed users from the restrictive cables, and has lead to a growing feeling of independence by being able to access the network services at anytime and from anywhere in their WLAN coverage areas.

WLAN technology has enjoyed remarkable growth in all aspects of life since the approval of IEEE 802.11, and since the introduction of wireless devices supporting that standard. WLANs now are found virtually in every location in the United States (U.S.), Europe, Japan and other countries around the world. In spite of the fact that the IEEE 802.11 standard was developed for indoor data exchange, the technology has been utilized to solve the last mile data exchange problem by extending WLAN boundaries to cover wider areas using the same equipments designed for indoor data exchange along with external antennas and signal amplifiers. Accordingly, many businesses, organizations and institutions around the world have begun to deploy WLANs for point-to-point and point-to-multi-points data exchange.

Since WLANs are flexible and modular in design, the technology is found to be used for different environments to meet the demand for mobile computing for small and large organizations. The technology also has been proven to be reliable for data exchange over long distances and many companies today use WLANs in widespread areas by bridging two or more WLANs/LANs using wireless routers. Furthermore, the technology is being used by *Wireless Internet Service Providers* (WISPs) around the U.S. and Europe to provide wireless broadband Internet access to their customers where fiber optics and other broadband services are not available.

Another segment of WLAN clients are the home users demanding freedom from cables and demanding the ability to share their broadband services throughout the house. Home users now can conveniently share computing resources such as printers, scanners and other highly priced devices. In order to extend the wireless broadband services to users who are traveling, service providers have started to install *Wireless Hotspots*, to be discussed in Chapter V, in public places such as airports, shopping malls, hotels, public parks and other public places. By using their notebook computers equipped with *Wireless Network Interface Cards* (WNIC), users can gain access to their corporate Intranets and the *World Wide Web* (WWW).

The WLAN technologies have achieved considerable thrust driven by user demand for freedom from cables and flexibility of expansion, which resulted in the continuation of standards updates and ratifications. Additionally, competition between manufacturers to develop wireless devices compatible with the newest and updated standards also resulted in high throughput, high performance and low price wireless.

B. OMAN'S TELECOMMUNICATION INFRASTRUCTURE

The Sultanate of Oman is considered to be one of the most advanced countries in the region in the telecommunications sector. It has enjoyed the newest in telecommunications technologies due to the rapid development of all technology sectors in the country. The country has one of the most advanced fixed and mobile digital telephone networks in the region. The network covers the country's major cities and towns as well as most of the mountainous, desert and the tropical southern regions.

Additionally, the country has an advanced fiber optics network that stretches for thousands of kilometers across the country and connects major cities and towns. Fiber optics facilities are still not available to normal users due to service prioritizations issues. Moreover, mobile (GSM) service, with a roaming agreement with more than 40 countries, covers not only major cities and towns; it also covers major highways, which stretch for thousands of kilometers across the country, also. The GSM service also provides text messages and low-speed Internet service connection for email services. Furthermore, thirty channel *Integrated Services Digital Network (ISDN)*, *Digital Circuits (DC)* and Internet *Dial-up* services have been available in Oman for a long time. In fact, Oman was one of the first countries in the region to introduce Internet service to the public.

Moreover, a large, recent plan exists to provide ADSL broadband service soon in the areas in and around the capital city. It is anticipated that other cities and regions will take longer time to enjoy the facilities of the new broadband service due to the widespread regions of the country. Thus, there is a real need for an alternative, quick and cost effective solution for providing broadband services to businesses, organizations, institutions and home users of other major cities and towns in Oman.



Figure 1. Map of the Sultanate of Oman.

C. OBJECTIVES OF THE THESIS

The goals of this thesis are to (1) solve the broadband service availability limitation in major Omani cities and towns by providing a design plan for a wireless network with different topologies and scenarios for businesses, organizations, institutions and home users, and (2) to provide a design plan for a wireless network for use by the military during both peacetime and operational time by providing a broad design for a wireless network in the field of operations.

D. METHODOLOGY OF THE THESIS

To accomplish the two objectives, the thesis will provide an in-depth study and review of wireless network technology and determine the fundamental building components of a wireless network. Next, the thesis will investigate the IEEE 802.11 family of standards and the wireless network design requirements. It will also examine the wireless network security problems to determine why wireless networks are more

vulnerable to hacking and attacks. It will review the available standards to support and enhance security functionalities and what measures to be taken in order to maximize the security level and minimize the adverse effects of an attack on a wireless network.

After determining the basic building blocks of a wireless network and understanding of the IEEE 802.11 wireless networks and security, market research will be conducted to find the available basic wireless network devices on the market that are compatible with the IEEE 802.11 standards.

Finally, the thesis will provide broad outlines of designing and implementing wireless networks for civilian and military applications mentioned in Section C.

E. THESIS ORGANIZATION

This thesis contains six chapters including the introduction.

Chapter II is a general overview of wireless network technology. This includes definitions, history, topologies, protocols, types, basic components and implementation considerations.

Chapter III describes the IEEE 802.11 family of standards including the history, architecture and services, Physical layer (PHY), Media Access Control layer (MAC) and IEEE 802.11 draft standards.

Chapter IV discusses wireless network security including security problems and vulnerabilities. At the end of the chapter, recommendations and guidelines are listed in order to improve the network security functionalities and elevate the security level.

Chapter V lists the results of market research conducted to identify the available basic required devices for the proposed wireless network including *Access Points* (APs), *Wireless Network Interface Cards* (WNICs), *Wireless Routers* (WRs) and external antennas. The chapter also outlines a design methodology approach for a civilian and military wireless network including a design plan for a wireless network for the Sultanate of Oman and military wireless network in the field.

Chapter VI concludes this thesis as well as summarizes the major points and findings of the thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WIRELESS NETWORKS TECHNOLOGY OVERVIEW

A. INTRODUCTION

This chapter will discuss the concepts of wireless networks in general, and Wireless Local Area Networks (WLAN) in particular, including a brief description of their history, topologies and components. At the end of the chapter, installation/deployment considerations, signal interference and other considerations and issues are discussed briefly.

B. WIRELESS NETWORK OVERVIEW

1. Definitions

A network is a flexible computer network that consists of two or more wireless stations connected to each other via airwaves instead of traditional cables and fiber optics. Wireless networks use electromagnetic airwaves, radio or infrared, to communicate information from one wireless station to another without any physical connections. Data is sent/received through the air, eliminating the need for wires, cables or any other physical media infrastructure. The main goal of wireless networks is to combine network connectivity, data availability and user mobility. [1]

Wireless networks are designed to look and feel like traditional wired networks so that no great differences between the two exists. Wireless networks support most of the protocols and LAN management tools designed to operate in an ordinary wired network.

2. History

During World War II, the United States Army developed a device to transmit data between two points by using radio signals. The data was encrypted and used to send war and battle plans to naval fleets and allies behind the enemy lines. Thus, wireless network technology goes back more than 50 years.

In 1971, utilizing WW II research done by the U.S. Army on radio data transmission, a group of researchers headed by Professor Norman Abramson at the University of Hawaii created the first Wireless Local Area Network (WLAN) using

packet communication through radio signals. The network was named ALOHNET and it linked seven computers, in a star topology, across four of the Hawaiian Islands.

In the following years, many wireless communications technologies, such as HiperLan2, Infrared, Home Radio Frequency (HomeRF), Wireless Application Protocol (WAP) and Bluetooth were developed. Since Infrared technology required a clear and direct line of site in a short distance, it has not been used widely when compared to radio technology. The other technologies using radio waves signals were in a better position to be developed rapidly, and the market was soon full of devices supporting these technologies. By using these devices, many Wireless Personal Area Networks (WPAN), Wireless Local Area Networks (WLAN) and Wireless Wide Area Networks (WWLAN) have been installed around the world to meet mobile computing requirements. [2]

Before 1990, WLAN equipment had not been standardized. Each manufacturer made its own protocols and standards for its devices and those devices were not able to communicate with devices made by other manufacturers.

In 1990, the Institute of Electrical and Electronics Engineers (IEEE) formed a working group, named 802.11, to standardize WLAN signaling and protocols. The standard took almost seven years to be accepted by the IEEE board in 1997. The IEEE 802.11 has become the first internationally recognized standard protocol for WLANs and vendors started to ship new products to support the newly accepted standard. [3]

The original IEEE 802.11-1997 standard operates on the 2.4 MHz frequency spectrum and supports 1-2 Mbps. In 1999, the standard was ratified to include two more new standards. These were named IEEE 802.11a operating on 5 MHz and supporting up to 54 Kbps, and IEEE 802.11b, operating on 2.4 MHz and supporting 11 Mbps. Vendors started to manufacture the IEEE 802.11b almost immediately since it is simpler than IEEE 802.11a. In early 2002, vendors started to ship products supporting either the IEEE 802.11a or IEEE 802.11b standard or both.

3. Topologies

There are two main types of WLAN topologies: the Ad-Hoc and the Infrastructure. In the Ad-Hoc WLAN topology, the network consists of stations within

short distances of each other to allow clear and strong signals to be transmitted between workstations. The communication between devices or workstations is done directly and by using Wireless Network Interface Cards (WNICs) with radio transceivers. WNICs convert the data to be transmitted to radio signals and re-convert back the radio signal to digital data at the receiving point through the WNIC card.

The Ad-hoc network has no specific structure, no fixed points and usually every node can communicate with every other node directly without any middle node. It is the simplest form of Wireless LANs and can be installed in a short time. This type of WLAN is sometimes called “Network on Demand” because it requires minimal planning, installations, configuration and administration.

To keep everything in order and under control in the Ad-Hoc WLAN, algorithms, such as the spokesman election algorithm (SEA), are used to elect one workstation as the base or the master station of the network and the rest of the stations as the slaves. The other algorithm used in the Ad-Hoc WLANs is a broadcast and flooding method to all workstations to identify who’s who in the network.

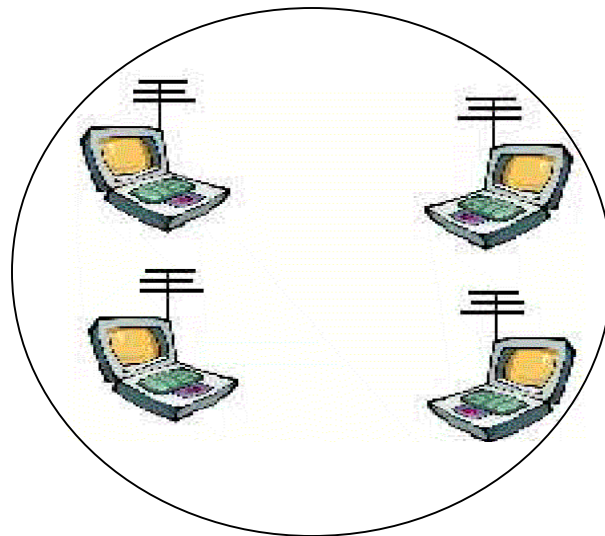


Figure 2. Ad-Hoc Wireless Local Area Network.

In the Infrastructure topologies, the network consists of the same WLAN devices found in the Ad-Hoc, such as wireless stations equipped with WNICs but in the Infrastructure topology, wireless workstations communicate with each other via a device

called an Access Point (AP), which acts as a controller. The AP can also act as a router to either another WLAN or to a traditional wired network expanding the scope of the entire network. In this form of WLAN, the stations do not have to be in range of each other, but they do have to be in range of at least one access point. This type of WLAN requires more planning, configuration and administration. By adding more APs and workstations, the Infrastructure WLAN can be expanded further to cover larger areas to meet the increasing demands for mobile computing by an organization. [3]

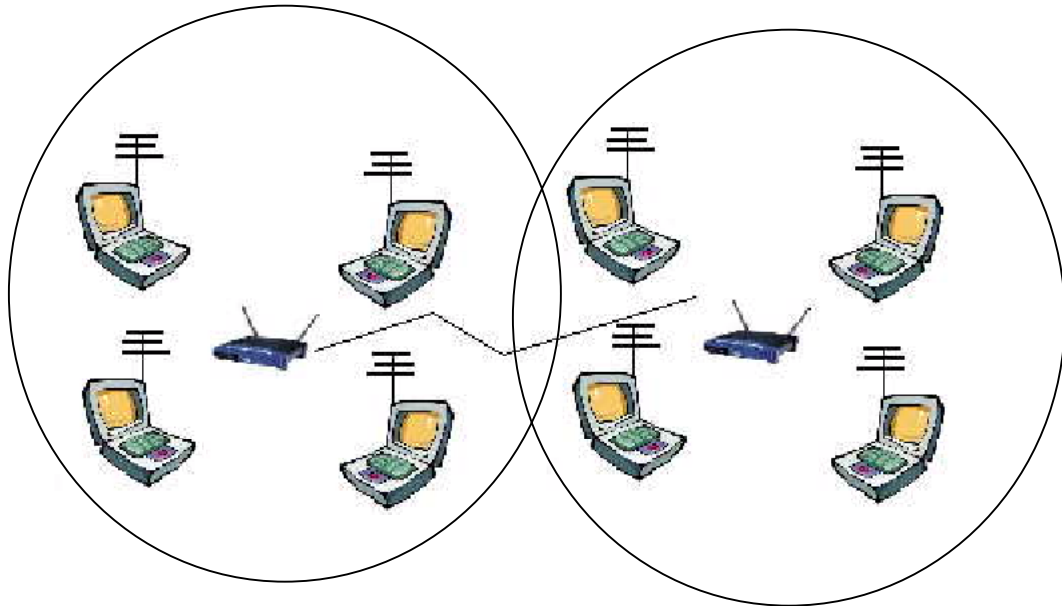


Figure 3. Infrastructure Wireless Network.

4. Protocols

A protocol is a set of special rules and conventions that standardize the method by which wireless devices such as workstations, Access Points (APs) and Wireless Network Interface Cards (WNIC) communicate with each other and that includes specifications on how data is encapsulated into message frames. The protocol also specifies the rules of data rates allowed, frequencies to be used, a request to send a message, an acknowledgement of receiving a message and other conventions.

As mentioned earlier, there are several wireless protocols and standards in existence today in the world, such as HiperLan2, Infrared, Home Radio Frequency (HomeRF), Wireless Application Protocol (WAP), Bluetooth and IEEE 802.11.

5. How Wireless Networks Work

Without using any physical connection, wireless networks, instead, use electromagnetic airwaves (radio/infrared) to communicate information from one station to another through the air. The airwaves sometimes are called carriers because they carry energy from the transmitting station (transmitter) to a remote receiving station (receiver).

So how is the data transmitted and received? The digital data to be transmitted is modulated on the radio waves (carrier) by the WNIC. The data modulated onto the radio carrier occupies more than one frequency because the frequency or bit rate of the modulated information adds to the carrier. More than one radio carrier can be used in the same space at the same time. These carriers do not interfere with each other because they are transmitted on different radio frequencies.

In order to receive the transmitted data at the other end, the receiver (WNIC) tunes in to the same radio frequency and rejects the other signals on different frequencies. The carrier is demodulated from the radio signal to digital data, which is delivered by the physical layer WNIC to the MAC layer and to the upper layers subsequently. [4]

6. Types

There are four major types of wireless networks: Wireless Personal Area Networks (WPAN), Wireless Local Area Networks (WLAN), Wireless Wide Area Networks (WWAN) and Wireless Metropolitan Area Networks (WMAN). A brief description of each type of these wireless networks follows.

a. Wireless Personal Area Network (WPAN)

A Wireless Personal Area Network (WPAN) is a small network interconnecting special purpose hand-held devices such as PDAs in a hospital, warehouse and other locations. The WPANs are also used for high-speed video/audio transfer from camcorders/digital cameras to televisions, projectors or personal storage devices. Further, they are used to transfer to and from printers, scanners and faxes. These devices are low-cost-low-power fixed, portable or moving within a Personal Operating Space (POS) of about 10 meters.

There are two major standards used for WPANs: the Bluetooth and the IEEE 802.15 family of standards. The Bluetooth standard was developed in Europe and it was the first wire replacement technology to allow interconnections of low-cost hand-held personal devices within the Personal Operating Space (POS). The standard offers a data transfer rate of 500~700 kbps, whereas the IEEE 802.15 family of standards, can achieve a data transfer rate of up to 55Mbps and is called High Data Rate Personal Area Networking. This speed is suitable for the wireless transfer of very large multimedia files, streaming video and audio such as MP3 in the POS in a short period of time. [5]



Figure 4. Wireless Personal Area Network (WPAN) [From: 5].

b. Wireless Local Area Networks (WLANs)

A Wireless Local Area Network (WLAN), in general, is a computer network that connects servers, desktop computers, notebooks, printers, scanners and other peripherals with each other through one or more Access Points (APs) by using airwaves instead of the physical infrastructure of cables or fiber optics as discussed earlier. These stations and peripherals are called Wireless Stations, or (STAs), for short. The STAs and APs are equipped with a Wireless Network Interface Adapter (WNIC) with radio transceivers. A description of APs and WNICs is given in more detail in the Wireless Network Components section. [6]

WLAN can cover a limited area and is mostly installed in one or more nearby buildings. WLAN users can share expensive devices, such as color laser printers, scanners and other devices. In addition, and the most important goal of a WLAN, is to make data and information available to authorized and privileged users across the network at any time.

Most WLANs installations today follow the Infrastructure topology due to their easy future expandability and flexibility. Some WLANs are linked to a wired network to expand their service and utilization.

c. Wide Wireless Area Networks (WWANs)

WWANs consist of two or more WLANs located mostly at long distances between each other and connected by a physical infrastructure or wireless network infrastructure. WWAN covers larger areas than WLAN and provides mobility for users across the network. By utilizing WWAN facilities, users can roam freely between the organization's offices across the country and around the world without having to carry any of the important work-related data files and information in their notebooks by minimizing the data security risks and physical damage to their notebook medias. [7]

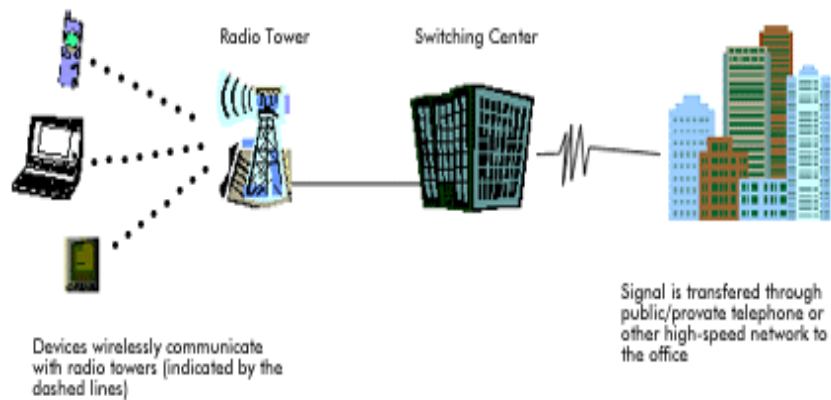


Figure 5. Wide Wireless Area Networks, [From: 7].

d. Wireless Metropolitan Area Networks (WMANs)

Another emerging wireless networks topology is the Wireless Metropolitan Area Network (WMAN), which provides a high-rate network connection path between a wireless subscriber site and stationary base network site. By using

amplifiers, the signal is boosted to travel longer distances on the same frequency, and by using external antennas, a signal can be directed to a specific location so that the receiving station can be located far away from the Access Point. The main goal of the WMAN is to provide businesses and homes a solution to the “last mile” problem and to gain access to the Internet through a local Wireless Internet Service Provider (WISP). [8]

A working group formed by the IEEE organization named the IEEE 802.16 workgroup was tasked to develop broadband wireless standards to solve the “last-mile” problem. The standard was published in April 2002 and it defines the WMAN air interface specifications on the licensed frequencies from 10 to 66 GHz with an intended speed from 2-155 Mbps. This spectrum is currently available worldwide. There have been a few suggested amendments to the original standard submitted by different sub-working groups and each addresses new issues and solves known challenges. [9]

Since the approval of the IEEE 802.11a and IEEE 802.11b standards in 1999, which use the 2.4 and 5 GHz license-free frequencies, and since the introduction of devices compatible with those standards to the market, numerous studies and test beds proved those devices could be used to build WMANs that provide wireless Internet access to homes and corporate users through a Wireless Internet Service Provider (WISP). Some of these WMANs can cover up to 30 miles from the base station with reasonable data rates. [10]

One example of WMAN installations is found at The High Performance Wireless Research and Education Network (HPWREN), based at the Supercomputer Center on the campus of the University of California, San Diego. It uses a long-shot of 72-miles-2.4-GHz wireless connection to San Clemente Island in the Pacific Ocean with a speed of 1 Mbps. The HPWREN has recently reduced the transmission power from 1 watt to 250 milliwatts in order to reduce the noise generated by the high 1-watt power in the surrounding areas of the campus after complaints made to the FCC. [11]

Today, many WISPs are found across the United States and around the world. These include the San Francisco Wireless Broadband, which is one of largest WISP in the United States, the Cleveland WISP, the Miami WISP and many more. To

serve the interests of the WISP's and ISP's worldwide, a non-profit organization was formed and named the Wireless Internet Service Provider Association. [12]

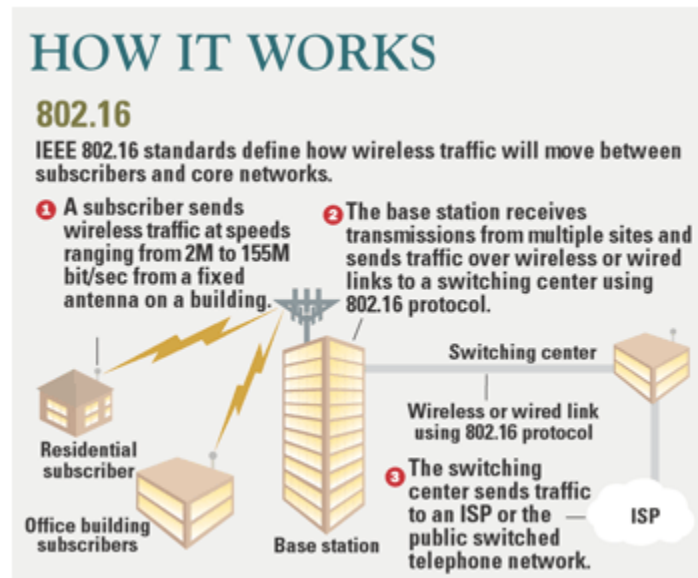


Figure 6. Wireless Metropolitan Area Networks, [From: 5].

So why are IEEE 802.11 compatible devices used for building WMANs when there is a specialized standard (IEEE 802.16) for WMAN configurations and communications? There are at least four reasons behind this. First, the IEEE 802.16 uses a licensed frequency spectrum (10-66 GHz) while the IEEE 802.11 uses license-free frequency spectrums (2.4 and 5 GHz). Second, the IEEE 802.16 standard was designed for fixed broadband base stations and requires a subscription to the service through local service providers, while the IEEE 802.11 wireless networks can be installed and used independently by anyone in almost any place in the world. Third, the greater design complexity of the IEEE 802.16 equipment compared to more simplified design requirements of the IEEE 802.11 devices attracted a few manufacturers to make those devices for IEEE 802.16. Finally, there are a few highly priced devices compatible with IEEE 802.16 available on the market today compared to more than 500 reasonably priced devices such as APs, WNIC/PCMCIA, antennas and amplifiers from many vendors compatible with the IEEE 802.11 family standards.

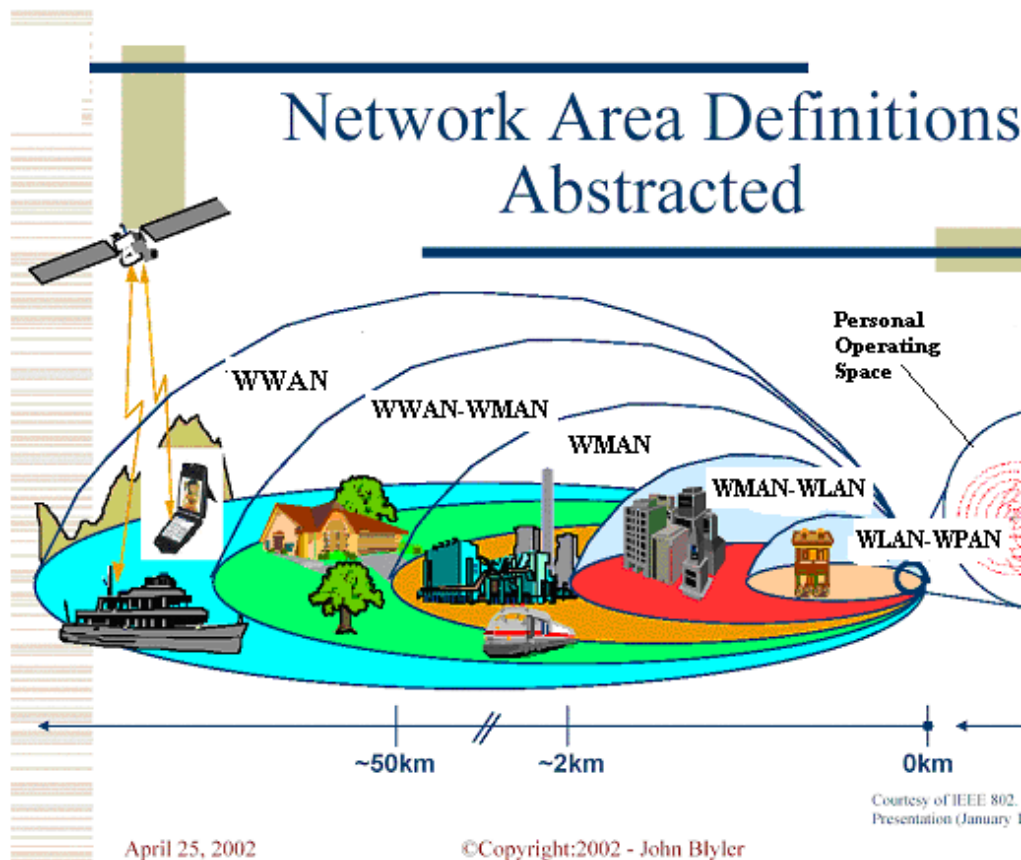


Figure 7. Network Types, [After: 13].

7. Basic Components and Operations of WLANs

In order to build a WLAN, a few devices and equipment are needed in addition to being somewhat knowledgeable of the terminology. The first basic component of any WLAN is the Cell, which is the smallest coverage area unit in the network. The total coverage area of a WLAN consists of one or more cells, and the coverage area of each cell depends on the radio signal strength, which is affected by physical obstacles such as walls, buildings, trees and mountains in addition to weather conditions and signal interferences. Without using any amplifiers or external antennas, the coverage area of each cell can range from 300 feet indoors to 800 feet outdoors.

The second component of a WLAN is the Access Point (AP) or 'Base Station', which is an electronic device used to manage communications in each cell. The AP communicates with all wireless stations in the cell and it also allows other wireless

stations in its coverage area to communicate with each other through it. The AP is also used as a relay station to extend the coverage area of the WLAN by bridging it with another WLANs, either wirelessly or by connecting it to a physical backbone of another WLAN or LAN. Each AP can support a small group of users, up to 64, within a range of a few hundred feet. The AP is usually equipped with a built-in antenna and it is mounted on a high wall or tower to cover a reasonable area. In order to expand the wireless network coverage area or to relieve a congested AP, more APs can be added to the network as needed. [14]



Figure 8. An Access Point (AP), [From: 15].

The third basic component of any wireless network is the Wireless Network Interface Card (WNIC), which is used by Stations (STAs) to communicate with other stations either directly or through an AP. WNICs usually come as adapter cards in desktop PCs, PCMCIA adapter cards for notebooks or are integrated with hand-held computers. The WNIC acts as an interface between the user Network Operating System (NOS) and the airwaves via an antenna. There are three main functionalities of the WNIC. The first is to provide the facility to detect, join/synchronize and authenticate with the WLAN. The second is to transmit/receive data in the form of frames from other stations in the WLAN, and the last is to encrypt/decrypt data being transmitted/received.

A WNIC establishes a connection with an AP with the strongest signal and it continues in connection with that AP until it detects another AP with a stronger signal while roaming between different cells or when the original AP is turned off. [14]



Figure 9. Desktop Wireless PCI Adapter, [From: 16].



Figure 10. Notebook Wireless PCMCIA Adapter, [From: 16].

There are two more wireless components used to direct and boost signal strength in order to expand the WLAN coverage area. These two components are antennas and amplifiers. An antenna takes radio frequency energy from the transmitter to the outside world and takes radio frequency energy from the outside world to the receiver. It also directs the maximum amount of energy to individual users within a cell. When a transmitter puts Radio Frequency (RF) energy in the form of a current into the sending station's antenna, the antenna responds by producing a magnetic field around the antenna. When this magnetic wave strikes the receiving station's antenna, it produces an electric current on the receiving antenna surface. The receiving station's receiver then converts the current to digital data.

There are two major types of antennas used for wireless networks today: Omni-Directional Antennas and Directional Antennas. The OmniDirectional antenna radiates the signal equally 360-degrees on a horizontal plane. There are several antennas that are considered to be OmniDirectional. Directional Antennas, also known as beam antennas, direct and concentrate the signal to a specific direction. There are many designs of the directional antennas and some of them date back to the 1920s, such as the Yagi directional antenna. [17]



Figure 11. Some of the Antennas Used For Wireless Networks, [From: 18].

Since most wireless devices such as WNICs and APs, use about +15 dBm power for transmission/reception, they cannot transmit/receive signals more than a few hundred feet indoors. To make the signal travel longer distances, a device named an amplifier is used to take the output signal from the WNIC/AP radio and amplify it with a certain amount of gain before delivering it to the external antenna. Amplifiers are usually installed between the Access Points and the antennas. A bi-directional amplifier can amplify the transmitted and received signals at different levels and is switched from receive to transmit by a certain level of Radio Frequency (RF) from the radio. Another type of amplifier is called a smart amplifier, which is a bi-directional amplifier that automatically reduces the transmit signal from the radio in order to preserve a steady output level. By using amplifiers, WLAN coverage can be extended to wider areas without using middle Access Points. [19]



Figure 12. Amplifier.

C. WHY DO WE USE WIRELESS NETWORKS?

It is known that traditional wired networks have been used for a very long time and have been proven to be very reliable, effective and more secure than wireless networks. In addition, the speed of traditional networks has been increasing steadily and significantly for the last few years, and today there are many gigabit networks installed around the world. So, why go back to slower and less secure networks with a data rate less than 100 Mbps for the fastest wireless network?

There are many benefits and advantages of the wireless networks that make them attractive to many companies, organizations and home users. One of the advantages is mobility, where users can access real-time information from anywhere and at anytime in their organizations resulting in higher productivity and service opportunities not possible with traditional networks. Another advantage is the installation speed; to install a WLAN is faster than installing a traditional network because it is not necessary to worry about laying physical complex cables, fiber optics or demolishing walls, which is time consuming and very costly. In addition to simplicity of installation; it is simpler to install a WLAN than to install a traditional network because it eliminates the need for cabling, ducting and other construction tasks, and with the new wireless device brilliant design, this can be a plug-and-play installation.

In addition to mobility, installation speed, installation simplicity, there is the benefit of less cost-of-ownership due to the dynamic corporate environment, which requires frequent moves. WLAN installations can reduce the cost of ownership of the WLAN. Corporations do not have to worry about moving cables to the new location and neither do they have to worry about cabling the new building to which they are moving.

The last advantage of WLAN is scalability. As organizations and companies expand, WLANs can grow as they grow by re-configuring the topologies to meet the demand for more network capacity and this can be done easily by adding more access points to accommodate more users. [4]

D. WIRELESS NETWORKS CONSIDERATIONS

In addition to the considerations taken for the installation of traditional computer networks, wireless networks installations require additional considerations. These include

physical location and weather considerations, signal interference, coverage area and compatibility/interoperability considerations. Furthermore, special considerations should be given to security, licensing and health issues. Some of these considerations are discussed below.

1. Physical Location and Weather Considerations

Special considerations should be taken into account when examining the physical location of both ends of the link. This includes structural support for antennas and lightning protection devices. Furthermore, any future planning for buildings, tree growth or other obstacles between the links should also be considered. Also, as with any other radio communication system, WLAN performance is affected dramatically by weather conditions. These conditions include, but are not limited to, heavy rain and fog, high winds, extreme temperatures and lightning. [20]

2. Signal Interference Considerations

Signal interference from other radio devices, within the network itself or from any other system in close proximity, is very important in the site survey planning. There are two types of radio interference that affect the transmission and reception of a radio link. The Co-Channel Interference is caused when another radio device uses the same channel frequency. The second type of the radio interferences is the Adjacent Channel Interference, which is caused when another device uses an adjacent channel frequency. To minimize the effect of radio interference, a device called a spectrum analyzer, is used to determine if any strong same or adjacent proposed channel signals are found in the planned installation site. If strong signals are found, the frequency must be changed to a higher or lower one.

3. Range, Coverage and Data Rate

Although the IEEE 802.11 family protocol standards do not specify the range and coverage areas of WLANs, many WLANs fail to meet the user expectations of reaching the alleged range claimed by some device manufacturers. The radius of coverage area for a typical WLAN varies from 100 feet to more than 300 feet, but even that cannot be achieved due to environmental and physical constraints. Regarding the data rate, the

IEEE 802.11 family of standards specified the data rate of a typical WLAN to range from 2 to 54 Mbps but there are many factors that affect the data rate, such as distance between the stations, the number of users on AP and the congestion on any wired network to which the WLAN is connected.

4. Compatibility and Interoperability

When planning to install a WLAN, special consideration must be given to the compatibility of the new network devices with the existing ones, and it is advisable to use the same standard hardware and software that is supported by the two networks, especially for the Network Operating System (NOS). Furthermore, and regardless of the fact that the IEEE 802.11 standards describe all the necessary rules, conventions and guidelines for the standardization and specifications of equipment, devices from different manufacturers may not be interoperable due to the differences in the design even if they both use the same technology.

5. Licensing Issues

The Federal Communications Commission (FCC) has approved specific unlicensed radio frequency spectrums with a maximum of 1-watt transmission power to be used in the United States for commercial, personal, scientific and medical wireless communications. These spectrums include 902 to 928 MHz, 2.4 to 2.483 GHz, 5.15 to 5.35 GHz, and 5.725 to 5.875 GHz. Wireless networks in the United States are designed to operate on these license-free frequencies. Any usage of any frequency not included in these unlicensed frequencies is subject to questioning by the FCC. [21]

When planning to deploy wireless networks in the Sultanate of Oman, licensing must be obtained from the Omani government.

6. Security Considerations

As with any new technology introduced to the market to solve problems, wireless networks technology was received enthusiastically by different types of companies and organizations especially after the approval of the IEEE 802.11 standard and the introduction of devices compatible with that standard. These devices have flooded the

market, and soon, companies and organizations were using them to build wireless networks for data exchange and mission critical applications.

Companies and organizations were under the false impression that their existing security measures used for their traditional wired Ethernet networks would be adequate for the newly installed wireless networks and would be able to maintain the same level of security. However, many vulnerabilities and security holes have been discovered in the IEEE 802.11 Wired Equivalent Protocol (WEP), which is the main security protocol for the IEEE 802.11. [20]

A more detailed discussion of wireless network security is provided in Chapter IV “Wireless Network Security”.

7. Health Issues

Since wireless network devices use radio waves to communicate between each other, several studies have been conducted to determine the negative effects of the emitted electromagnetic energy from those devices. The studies found that users do not suffer any ill effects from these devices since they have been designed to operate within guidelines found in radio frequency safety standards and recommendations which are continually reviewed by panels and scientists, such as the Standards Coordinating Committee 28 of the Institute of Electrical and Electronics Engineers (IEEE), the National Council on Radiation Protection and Measurements (NCRP), the National Radiological Protection Boards (NRPB) in the United Kingdom and the International Radiation Protection Association's International Non-Ionizing Radiation Committee (IRPA/INIRC) which is under the sponsorship of the World Health Organization. [22]

E. SUMMARY

This chapter introduced the wireless network technologies and included the history, topologies, protocols and advantages over wired networks. The chapter also discussed the considerations to be taken in order to successfully deploy a wireless network, including the weather, signal interference and other considerations.

A detailed discussion of the IEEE 802.11 family of standards will be presented in the next chapter to demonstrate how these standards were developed, evolved and

dominated wireless network standards. In addition, the chapter will analyze the Physical (PHY) and Media Access Control (MAC) layers and sublayers to show their characteristics and services. Finally, a brief description of the recent IEEE 802.11 task forces will be provided.

III. OVERVIEW OF IEEE 802.11 STANDARD

A. INTRODUCTION

In the previous chapter, reviews of the history, topologies, components and operations, types and deployment considerations of WLANs were given to show WLAN technology evolution and importance in our lives.

This chapter will introduce and analyze the IEEE 802.11 family of standards, the first internationally recognized *Wireless Local Area Network* (WLAN) standards. The discussion will cover the IEEE 802.11 history, architecture, Physical (PHY) and *Media Access Control* (MAC) layers and sublayers to analysis their characteristics, functions and the design requirements for the devices compliant with these layers. At the end of the chapter, a brief description of the IEEE 802.11 standards still under development is given to show what can be expected in the near future. This analysis will concentrate on the *Radio Frequency* (RF) technology and does not discuss the Infrared technology since the Infrared devices are very limited in the market as they require direct point of sight. Accordingly, most of the IEEE 802.11 devices introduced in the market today support the Radio Physical layers.

B. HISTORY

The IEEE committee adopted the IEEE 802.11 standard in 1997 after a long period of development lasting more than five years. The goal of this standard is to provide wireless interconnection between devices and equipment that require fast installation and deployment along with mobility.

The original IEEE 802.11-1997 standard defines the Media Access Control layer (MAC) and three *Physical layers* (PHY) for wireless connectivity. These three Physical layers are the *InfraRed* (IR), the *Frequency Hopping Spread Spectrum* (FHSS) and the *Direct Sequence Spread Spectrum* (DSSS). All three Physical layers in the IEEE 802.11-1997 operate in the unlicensed 2.4 frequency spectrum with data rate ranges from 1 Mbps up to 2 Mbps. The IEEE 802.11-1997 standard was revised in 1999 to include two new radio Physical layers: the IEEE 802.11a-1999 operating at the license free 5 GHz frequency spectrum with data rates up to 54 Mbps and the IEEE 802.11b-1999 which

operates in the unlicensed 2.4 GHz frequency spectrum with data rates up to 11 Mbps. The MAC layer of the IEEE 802.11-1999 remained the same as that of the original IEEE 802.11-1997 with minor improvements. [23]

Although the IEEE 802.11 standard was originally developed for medical, educational and home usage, it has opportunely been used by companies and organizations for wireless data exchange since it uses unlicensed frequency spectrums that require no licensing from the *Federal Communication Commission* (FCC). FCC is an independent U.S. government agency governing all communication frequencies in the U.S. Details of those unlicensed frequency are discussed later in the chapter.

C. IEEE 802.11 ARCHITECTURE AND SERVICES

The IEEE 802.11 architecture consists of a number of components and services that interact with each other to provide station mobility transparency to higher layers of the network stack. The IEEE 802.11 services include the *Basic Service Set* (BSS) and the *Extended Service Set* (ESS). The BSS consists of *Stations* (STAs) located in close proximity and communicate directly with each other by airwaves without relay stations. The maximum allowed distance between stations is determined by the electromagnetic propagation and signal interference, which affects the signal strength and data rate. If no *Access Point* (AP) is utilized, this type of architecture is called *Independent Basic Service Set* (IBSS), otherwise, it is called *Infrastructure*. The Ad-hoc and the Infrastructure WLANs, discussed in the previous chapter, use one form or another of this service set. The ESS is used to extend the range and the coverage area of a WLAN by connecting it to one or more infrastructure BSSs of the WLANs with one or more APs. For wired networks in communication with a WLAN, the ESS and its mobile STAs, look like one MAC-layer network and all the STAs appear to be stationary. In other words, the wireless connectivity is hidden from other wired networks to which it is connected. [23]

Access Points communicate with each other to coordinate and forward traffic between themselves and between STAs. Communication between APs is carried by an abstract medium named the *Distribution System* (DS), which is the technique, or the mechanism used to connect BSSs through APs acting as the backbone of the WLAN and

could be built of wired or wireless networks. The DS is a thin layer in the AP responsible for determining where the received traffic is to be forwarded.

In order to provide functionalities for the DS, the IEEE 802.11 included five distributed services to the MAC layer architecture. The DS functionalities are carried out by APs when exchanging frames between other APs or STAs. The five distribution services and functions are Association, Disassociation, Distribution, Integration and Reassociation.

In addition to the DS, there are four *Stations Services* (SS) specified for use by the MAC layer and the purpose of these services is to provide security and data delivery services for the WLAN. The four SSs are authentication, de-authentication, privacy and delivery. [24]

The Distributed Services and the Station Services are discussed in the MAC layer section of this chapter.

D. IEEE 802.11 PHYSICAL LAYER (PHY)

The IEEE 802.11 *Physical Layer* (PHY) is located at the bottom of the *Network Protocol Stack* (NPS). There are three main functions of the PHY layer. The first function is to provide an interface to exchange frames with the MAC layer for the transmission and reception of data. The second function is to use signal carrier and *Spread Spectrum* modulation (SS) to transmit data frames over the media. The modulation enables several devices to share radio frequencies concurrently, without interfering with each other and is considered to be an efficient way of using radio waves to communicate. The last function of the PHY layer is to provide a carrier sense indication back to the MAC to verify activity on the media. [24]

This *Spread Spectrum* modulation technique (SS) was originally developed during WW II by a talented Hollywood Star named Lamarr Mandl's, who was Fritz Mandl's wife. Fritz Mandl was one of Europe's largest armaments manufacturers. The SS technology was developed further by the U.S. military to prevent jamming and interception of military and intelligence signals by spreading the information signal over a wider bandwidth. [25]

Application
TCP, UDP
Network/Internet (IP)
Data Link MAC (CSMA/CA)
Physical (FH,DSSS,HRDSSS,OFDM)

Figure 13. MAC And Physical Layers Location.

The IEEE 802.11-1997 standard has two different Physical layer specifications for *Radio Frequency* (FR) and one physical layer for *Infrared* (IR). The two radio physical layers are *Frequency Hopping Spread Spectrum* (FHSS) and *Direct Sequence Spread Spectrum* (DSSS). Each PHY standard operates on 1 Mbps and a 2 Mbps rate mode. Further, each PHY layer is divided into two sublayers, the *Physical Layer Convergence Procedure* (PLCP) sublayer, which simplifies the interface to the MAC, and the *Physical Medium Dependent* (PMD) sublayer, which provides transmission, reception and a channel assessment. [23]

To meet the demand for higher data rates, the IEEE 802.11 organization amended the IEEE 802.11-1997 Physical Layer to include two more new RF Physical Layers in addition to the three other physical layers (DSSS, FHSS and IR). These two newest physical layers are *the Orthogonal Frequency Division Multiplexing* (OFDM) and *High Rate Direct Sequence Spectrum* (HRDSSS) PHY, and the amended standards were named IEEE 802.11a and IEEE 802.11 b. The IEEE 802.11a, which uses the OFDM modulation, operates on the 5 MHz frequencies and can achieve up to 54 Mbps. The IEEE 802.11b uses the HRDSSS and operates on the 2.4 MHz frequency, and can achieve up to 11 Mbps. In the following sections, the four Physical Layers, DSSS, FHSS, IEEE 802.11a (OFDM) and IEEE 802.11b (HRDSSS), are discussed to show their major characteristics and sub-layers.

1. Direct Sequence Spread Spectrum Physical Layer (DSSS)

By fragmenting the base-band signal at 11 MHz with an 11-chip PN code, the DSSS system provides a processing gain of at least 10 dB according to FCC regulations. The DSSS system uses baseband modulations of *Differential Binary Phase Shift Keying* (DBPSK) and differential *Quadrature Phase Shift Keying* (DQPSK) to provide the 1 Mbps and 2 Mbps data rates, respectively. [23]

The original IEEE 802.11-1997 DSSS PHY layer consists of two sublayer protocol functions. The first function is the physical layer convergence function, which helps the *Physical Medium Dependent* (PMD) system adjust to the PHY service. This function is controlled by the *Physical Layer Convergence Procedure* (PLCP) that defines a method for mapping the IEEE 802.11 MAC sublayer *Protocol Data Unit* (PDU) into a framing format appropriate for sending/receiving data and management information between stations using the associated PMD system.

The second function of the DSSS PHY is the *Physical Medium Dependent* (PMD) function, which defines the characteristics and method of transmitting/receiving data through a *Wireless Medium* (WM) between stations. [23]

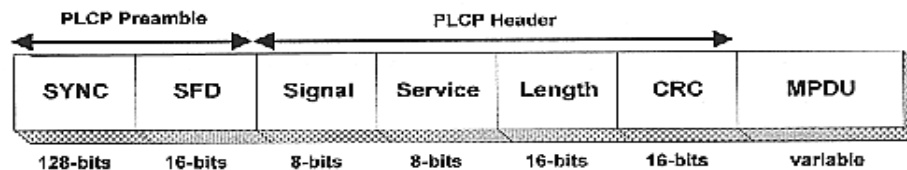


Figure 14. PLCP Frame Format [From: 24].

2. Frequency Hopping Spread Spectrum (FHSS)

The basic idea of a *Frequency Hopping Spread Spectrum* (FHSS) is to change frequency constantly in random patterns by using a different frequency each time or hopping from one channel to another. During hopping, the *Physical Medium Dependent* (PMD) transmits frames at one frequency for a specific time, called the dwell, and then “hops” to a new channel to transmit for the next dwell period.

The transmission frequencies are determined by a spreading/hopping code. The receiver must be adjusted to the same hopping code and must listen to the incoming

signal at the right time and the correct frequency in order to successfully receive the signal. This technique is used to reduce interference with other radio sources since a signal from a narrowband system will only affect the spread spectrum signal if both are transmitting at the same frequency at the same time. The IEEE 802.11 standard defines different sets of channels to shift between different parts of the world. When using a specific frequency, FHSS modulates a logical 1 by raising the frequency. In order to send a logical 0, FHSS lowers the frequency. This modulation design is used when transmitting with 1 Mbps. Four different levels are used when raising the bandwidth to 2 Mbps, each representing 2 bits. The maximum bandwidth of FHSS is 2 Mbps, but for some non-standard products, 3 Mbps throughput was achieved.

The signal transmitted with FHSS has greater bandwidth than the signal transmitted with fixed frequency and it is less vulnerable to interception. The technique uses a complicated mathematical function of time, and the hacker must know the exact frequency versus time used by the transmitter besides knowing the exact starting point of the function.

Similarly to the DSSS PHY, the FHSS PHY consists of two protocol functions. The first function is the Physical Layer Convergence (PLC) function, which helps the *Physical Medium Dependent* (PMD) system to adjust to the PHY service. This function is controlled by the *Physical Layer Convergence Procedure* (PLCP), which defines a way of mapping the IEEE 802.11 MAC sublayer *Protocol Data Units* (PDUs) into a framing format appropriate for sending/receiving data and management information between stations using the associated PMD system.

The second function of the FHSS PHY, as with that of the DSSS PHY, is the *Physical Medium Dependent* (PMD) function, which defines the characteristics and method of transmitting/receiving data through a *Wireless Medium* (WM) between stations. [23]

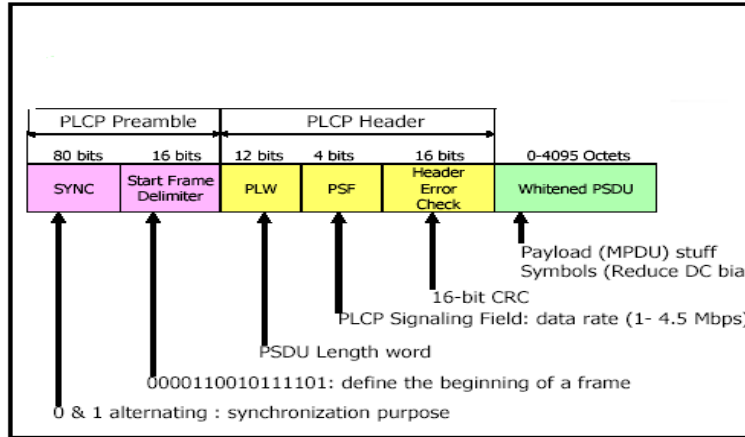


Figure 15. FHSS PLCP Frame Format.

3. IEEE 802.11a

The IEEE 802.11a standard uses the *Orthogonal Frequency Division Multiplexing* (OFDM) modulation technique. This modulation technique divides the data signal across 48 separate sub-carriers in order to provide transmissions of 6, 9, 12, 18, 24, 36, 48, or 54Mbps. The 6, 12, and 24Mbps were made mandatory for all products compliant with the IEEE 802.11a. The OFDM uses *Phase Shift Keying* (PSK) or *Quadrature Amplitude Modulation* (QAM) to modulate the signal depending on the selected data rate of transmission. Furthermore, four of the subcarriers are pilot subcarriers used as a reference to disregard frequency or phase shifts of the signal during transmission. [24]

a. PLCP DATA Scrambler

The DATA field, which consists of the SERVICE, PSDU, tail, and pad fields, is scrambled with a length-127 frame-synchronous scrambler. The contents of the PSDU are placed in the transmit serial bit stream. Bit 0 is placed first in the stream and bit 7 in the last. The frame synchronous scrambler uses the generator polynomial:

$$G(x) = x^7 + x^4 + 1$$

b. OFDM Modulation

In the OFDM modulation, many lower-speed subcarriers are combined to form one high-speed channel to achieve a high data rate. A wide channel can transport more information per transmission than a narrow one. The OFDM protocol defines eight non-overlapping channels of 20 MHz each across the two lower bands. Each of these

channels is divided into 52 subcarriers of about 300 KHz wide each. Each narrowband subcarrier is modulated using BPSK, QPSK or *Quadrature Amplitude Modulation* (QAM) and then all subcarriers are transmitted in parallel and received simultaneously. The receiver processes each individual signal, which represents a portion of the total data. All received signals are combined together to create the actual signal. [24]

In order to overcome the high data errors due to high data rate transmission, IEEE 802.11a had to be equipped with an error correction algorithm. The algorithm was named the *Forward Error Correction* (FEC). The basic idea of this error correction algorithm is to send a second copy of the primary information. If part of the primary information is lost, then the receiving station can recover the lost data through sophisticated algorithms. If part of the signal is lost, the information can be recovered eliminating the need for the retransmission of the data. [23]

c. IEEE 802.11a Operating Channel Frequencies Range

The FCC has allocated 300 MHz of bandwidth in the 5 GHz *Unlicensed National Information Infrastructure* (U-NII) band for IEEE 802.11a operations in the U.S. The total 300 MHz is divided into three different 100 MHz domains, each with a different legal maximum power output. These bands are low, middle and high band. The low band operates from 5.15 – 5.25 GHz, and has a maximum of 50 milliwatts. The middle band is from 5.25 – 5.35 GHz, with a maximum of 250 milliwatts. The high band utilizes the 5.725 – 5.825 GHz, with a maximum of 1 Watt. [23]

Regulatory domain	Band (GHz)	Operating channel numbers	Channel center frequencies (MHz)
United States	U-NII lower band (5.15–5.25)	36	5180
		40	5200
		44	5220
		48	5240
United States	U-NII middle band (5.25–5.35)	52	5260
		56	5280
		60	5300
		64	5320
United States	U-NII upper band (5.725–5.825)	149	5745
		153	5765
		157	5785
		161	5805

Table 1. 5 GHz Operating Channels [From: 23].

4. IEEE 802.11b

This physical layer was approved in September 1999 as IEEE 802.11b and it was an addendum to the original IEEE 802.11 as a higher-speed physical layer extension in the 2.4 GHz band. It is called the *High Rate DSSS PHY Layer* (HRDSSS) and it introduced new features and capabilities, and expands the data rates provided by the original standard. The extension adds data rates of 5.5 and 11 Mbps to the existing rates of 1 and 2 Mbps. To achieve that high rate, it requires the implementation of an 8-chip *Complementary Code Keying* (CCK) in combination with the 11-bit chipping code of the *Direct Sequence Spread Spectrum System* (DSSS). The implementation of CCK resulted in the ability to transmit 4 bits of data for each transmitted symbol for 5.5 Mbps and 8 bits of data per symbol for 11 Mbps

The IEEE 802.11b protocol specifies dynamic rate shifting to allow data rates to be automatically adjusted for noisy environments. The IEEE 802.11b devices transmit at lower speeds of 5.5Mbps, 2Mbps and 1Mbps under noisy surroundings. When the noise decreases, the devices increase the data rate automatically.

Data Rate	Code Length	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11 (Barker Sequence)	BPSK	1 MSps	1
2 Mbps	11 (Barker Sequence)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

Table 2. IEEE 802.11b Data Rate Specifications [From: 23].

a. IEEE 802.11b Operating Channel Frequency Range

The HRDSSS PHY operates in the 2.4–2.4835 GHz frequency range in the U.S., Canada and Europe. On the other hand, France allows operation from 2.4465–2.4835 GHz, and Spain allows operation from 2.445–2.475 GHz. For Japan, the 2.471–2.497 GHz frequency range is specified for operation. Table 3 shows the HRDSS frequency channel range. [23]

CHNL_ID	Frequency (MHz)	Regulatory domains					
		X'10' FCC	X'20' IC	X'30' ETSI	X'31' Spain	X'32' France	X'40' MKK
1	2412	X	X	X	—	—	—
2	2417	X	X	X	—	—	—
3	2422	X	X	X	—	—	—
4	2427	X	X	X	—	—	—
5	2432	X	X	X	—	—	—
6	2437	X	X	X	—	—	—
7	2442	X	X	X	—	—	—
8	2447	X	X	X	—	—	—
9	2452	X	X	X	—	—	—
10	2457	X	X	X	X	X	—
11	2462	X	X	X	X	X	—
12	2467	—	—	X	—	X	—
13	2472	—	—	X	—	X	—
14	2484	—	—	—	—	—	X

Table 3. High Rate PHY Frequency Channel Plan [From: 24].

b. IEEE 802.11b Modulation and Channel Data Rates

There are four modulation formats and data rates specified for the HRDSSS PHY: basic, enhanced, extended and high rate access rates. The basic access rate is based on the 1 Mbps *Differential Phase Shift Keying (DPSK)* modulation. The enhanced access rate is based on the 2 Mbps DQPSK. The extended direct sequence specification defines two additional data rates whereas the *High Rate* access rates are based on the CCK modulation system for 5.5 Mbps and 11 Mbps. [23]

E. IEEE 802.11 MEDIA ACCESS CONTROL LAYER (MAC)

The Medium Access Control (MAC) layer of the IEEE 802.11 provides the functionalities that are needed to deliver data over noisy and unpredictable wireless media. There are three main MAC functionalities specified by the IEEE 802.11 standard. The first is to provide reliable data delivery services to the users of the MAC. The second is to manage access to the common wireless medium by using two different access mechanisms. The basic access mechanism is called *Distributed Coordination Function (DCF)* and the centrally controlled access mechanism is called the *Point Coordination*

Function (PCF). The third function of the MAC layer is to provide security for the data that it delivers.

In the following sections, a brief description of the primary access method of the IEEE 802.11 MAC, MAC services and the MAC frame exchange protocol, are discussed to explain how MAC delivers data by the “best effort” method. [23]

1. Basic Access Method (CSMA/CA)

The primary access method of the IEEE 802.11 MAC is called *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA). The CSMA/CA is implemented in all STAs for use within both *Independent Basic Service Set* (IBSS), and Infrastructure network topologies. In order for a STA to send a packet, it first senses the medium to ascertain if another STA is transmitting at that point in time. The STA must ensure that the medium is unused for the required period before starting to transmit. If the medium is found to be busy, the STA waits until the end of the recent transmission. The STA selects a random backoff interval and decrements the backoff interval counter while the medium is idle. When the medium is free for transmission, the STA first sends a *Request To Send* (RTS) frame to the AP before each data frame is transmitted. In return, the AP sends back a *Clear To Send* (CTS) frame allowing the station to send its frame. The frame that is sent by the AP and received by all workstations has the time that the specific station has allowed for transmission. The other STA cannot transmit during that period regardless of the fact that the medium appears to be free. A brief description of the MAC frames and their sub types are given in the next section. [23]

2. MAC Frames

There are three types of frames generated by the MAC layer: the *Data Frames* used for data transmission, the *Control Frames* used to control access to the medium and the *Management Frames* used to exchange management information between MAC layers of the communicating STAs. Each MAC frame consists of a MAC header, a variable length frame body and a *Frame Check Sequence* (FCS). The MAC header comprises a frame control, duration address and sequence control information. The variable length frame body has information particular to the frame type.

The MAC general frame format consists of different fields that occur in a specific order in all frames. These fields are *Frame Control*, *Duration/ID*, *Address 1*, *Address 2*, *Address 3*, *Sequence Control*, *Address 4*, *Frame Body* and *Frame Check Sequence (FCS)*.

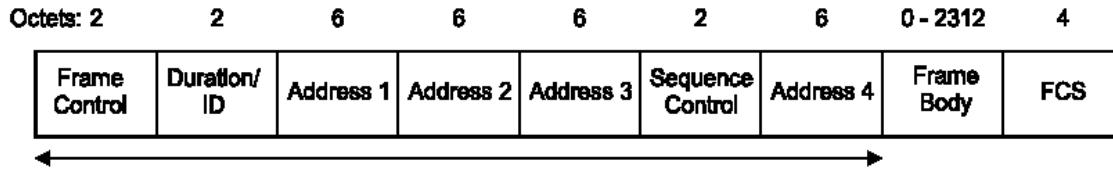


Figure 16. MAC General Frame Format [From: 23].

a. Control Frames

The control frame has six control frames subtypes. The three main control frames subtypes are *Request To Send (RTS)*, *Clear To Send (CTS)* and *Acknowledge (ACK)*.

The RTS frame used when a station wants to send a data frame to another station. The RTS is the first part of a two-way handshake communication. This function reduces frame collisions when more than one station is associated with one AP.

The CTS frame is used when a station receives an RTS frame indicating that it is ready to receive the transmission from the sending station. The CTS Frame has a time value to inform other stations not to send any frames during that period which should be enough for the requesting station to send its frame.

The receiving station sends the ACK frame to the sending station when the data frame is received error free. The sending station waits for a period of time to receive the ACK frame, and if it does not receive it within that period of time, it resends the same frame. [23]

b. Management Frames

The IEEE 802.11 MAC layer defines wide frame management facilities through the management frames. The management frames are responsible for setting up and preserving communications between workstations and APs. All management frames have frame control, duration, address 1, address 2, address 3, sequence number, frame body and *Frame Check Sequence (FCS)*. Some of the important management frames are

Beacon, Authentication, De-Authentication, Association Request, Association Response, Disassociation and Probe Request Frame.

The Beacon frame is sent by APs periodically to announce their existence to all STAs within range. They contain information about the APs such as timestamp, SSID and other parameters. At the same time, STAs continually scan all channels and listen to APs signals to choose the best with which to associate.

The Authentication frame is sent by the STA to an AP with which it desires to associate, and the frame contains the STA identity. On the other hand, the De-Authentication frame is sent by a station to terminate a connection.

The Association Request frame is sent by the STA to the AP to allocate resources and synchronize with it. First, the STA sends an association request to the AP providing information about the STA such as data rates and the *Service Set Identifier* (SSID) of the network with which it wishes to associate. In return, the AP sends the Association Response frame containing an acceptance or rejection notice to the STA that requested the association. If the Association Request was accepted, then the association response frame will contain the association ID for the STA and supported data rate. The AP also reserves memory space for the transaction and adds it to the association table. The STA can utilize the AP for any connection with other STAs on the network.

The Re-Association Request frame is sent by a roaming STA currently associated with an AP when it finds another AP with a stronger signal. This frame is sent to the new AP, which in return, coordinates with the old AP to forward the data still in its buffer for the STA.

The Re-Association Response frame is sent by the new AP that received the Re-Association Request frame to the requested STA. It contains an acceptance or rejection notice. If the Re-association Response frame contains an acceptance notice, then it also contains the association ID and supported data rates.

The Disassociation frame is sent by a STA that wishes to disassociate itself from an AP or another STA for any reason, which in return, deletes it from the association table and frees the allocated memory.

Finally, the Probe Request frames are sent by STAs to obtain information from other stations within range to know which stations are live. In return, the stations within range send a Probe Response frame with capability information, supported data rates and other information. [26]

c. Data Frames

The Data frame is independent of subtype, variable in length and ranges from a minimum of 29 to a maximum of 2346 bytes. Further, the content of the Address fields in the data frame is dependent upon the values of the To DS and From DS bits and as shown in Table 4. Address 1 of the frame contains the receiver address of the intended receiver or the address of multicast frames receivers. Address 2 contains the address of the station that is transmitting the frame.

The frame body consists of the MAC Service Data Unit (MSDU) and a WEP Initial Vector (IV) and ICV if the WEP subfield in the frame control field is set to 1.

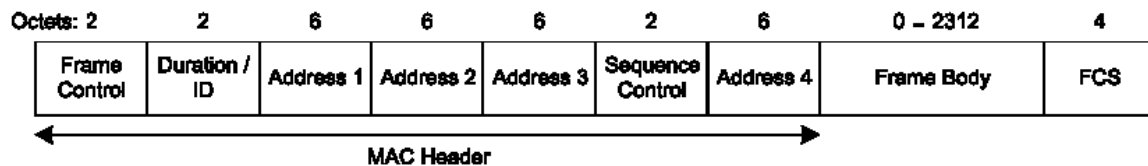


Figure 17. Data Frame Format [From: 24].

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Table 4. Data Frame Address Field Contents [From: 24].

F. IEEE 802.11 DRAFT STANDARDS

Some of the newly IEEE workgroups formed to enhance the IEEE 802.11 security, backward compatibility and quality of service are discussed below.

1. IEEE 802.11g

Since IEEE 802.11a and IEEE 802.11b operate in two different frequency spectrums (2.4 and 5 GHz), the devices are not compatible with each other. Thus, companies and organization invested in IEEE 802.11b could loose their investment if they decided to move to the IEEE 802.11a standard having a higher data rate.

To solve the backwards compatibility problem with IEEE 802.11b, the IEEE formed a working group to study the problem and draft a standard to be followed by manufacturers to design devices that could achieve a data rate of 54 Mbps and still be compatible with the IEEE 802.11b devices. The workgroup was named IEEE 802.11g. The new standard operates in the 2.4 GHz of the IEEE 802.11b but uses the same OFDM format as the IEEE 802.11a and delivers a speed of up to 54 Mbps.

In late 2002, the IEEE committee approved IEEE 802.11g and manufacturers began to ship the new compatible devices as early as January 2003. One of the first devices introduced to the market was the AirPort Extreme Base Station with a modem and antenna port from Apple Computers.

2. IEEE 802.11e (Quality of Service)

The IEEE 802.11e task force group was formed to draft an amendment to the IEEE 802.11 family standards to enhance the capabilities and efficiency of the current MAC layer, which has not been amended since the approval of the IEEE 802.11-1997, including quality of service requirements. The new and enhanced capabilities of the MAC layer will expand the IEEE 802.11 application services and quality resulting in high clarity and reliability of voice, audio and video streaming in addition to video conferencing. The standard will use a technique called Hybrid Coordination Function (HCF). The final approval of this standard is expected within the first half of this year (2003).

3. Other IEEE 802.11 Draft Standards

The IEEE organization has formed more task forces to develop and enhance the current IEEE 802.11 family of standards. One task force was named IEEE 802.11c to improve bridge functionality between IEEE 802.11 WLANS and traditional wired LANs.

Another task force was IEEE 802.11d and it is concerned with devices specifications to configure themselves properly to be able to operate anywhere in the world. In addition, the IEEE 802.11h task force was formed to look into Spectrum and Power Management extensions in the 5 GHz band for outdoor use in Europe, which is equivalent to the IEEE 802.11a in the United States. Furthermore, IEEE 802.11i was formed to enhance the security specifications of the IEEE 802.11 family and it would eventually replace the current WEP encryption with a new algorithm named the Advanced Encryption Standard (AES). The standard will use the IEEE 802.1x (Port-Based Network Access Control) standard as the authentication mechanism protocol. [3-5]

G. SUMMARY

This chapter discussed the IEEE 802.11 standard to explain how it has evolved to become the dominant wireless network standard in the world by going through different development stages. The chapter also described the IEEE 802.11 architectures, services and specifications to understand the characteristics and functions of the *Physical* (PHY) and the *Medium Access Control* (MAC) layers and sub-layers. Finally, a brief description was provided of the recent IEEE 802.11 draft standards.

The next chapter will analyze the wireless network security and vulnerabilities and will examine the techniques used to protect and encrypt/decrypt the data being exchanged between different wireless stations. At the end of the chapter, a list of recommendations is provided in order to increase the security level of a wireless network.

IV. WIRELESS NETWORK SECURITY

A. INTRODUCTION

In the previous chapter, IEEE 802.11 family of standards was introduced. This chapter will demonstrate the wireless network problems, attacks, algorithms and improvements to the wireless network security. Additionally, the chapter will list recommendations for improving the wireless network security and reducing the vulnerabilities of the network.

As with any other new technology developed to help solve any problems in our lives, companies, organizations and individuals enthusiastically received wireless networks technology, especially after the approval of IEEE 802.11 and the introduction of devices compatible with that standard. These devices have flooded the market and soon companies and organizations were using them for imperative data exchange and mission critical applications.

At first, companies and organizations did not take wireless network security issues seriously, and they continued to follow the same security policies and measures developed for their existing traditional wired Ethernet networks, which were demonstrated to be inadequate for Wireless Networks due to the open space they use as the medium of transmission compared to the closed wired medium. As the deployments of Wireless Networks increased, many vulnerabilities and security holes have been discovered in the IEEE 802.11 Wired Equivalent Protocol (WEP), which is the main security protocol for IEEE 802.11.

In early 2001, a task team at UC Berkeley discovered serious flaws in the IEEE 802.11 WEP algorithm implementation that allowed the decryption of traffic by analyzing intercepted packets. The team was also able to inject packets into the traffic from unauthorized mobile stations. Moreover, the team was successful in tricking Access Points by decrypting intercepted data. Finally, the team was able to automate the decryption in real time after they built a dictionary of just one day's traffic. [4-1]

There were many documented cases, in addition to those at the University of California at Berkeley, where Wireless Network security has been compromised when

hackers used mobile Wireless Stations equipped with parabolic dishes in parking lots to intercept Wireless Network signals. This is called “**War driving**”. The hackers used software packages that analyzed and decrypted the collected data to comprehend the authentication keys, and when that was successfully completed, they had everything. This method is known as “authentication spoofing”.

B. PROBLEMS WITH WIRELESS NETWORKS SECURITY

Wireless Networks have been subject to numerous kinds of attacks because they are not contained to specific physical borders when exchanging data between stations. They use the airwaves that are open to anyone who listens and can record almost any transmission for further analysis. The following are some factors that made Wireless Networks attractive to hackers for different purposes.

1. Easy Access

In order for Wireless LANs to allow accessibility to legitimate users, Wireless Stations (STAs) and Access Points (APs), in most cases, need to announce their presence in the airwaves so users, through other STAs, can access the network for different authorized services. The STAs and APs announce their presence by sending special frames called Beacons. These frames are transmitted in open air without any privacy functions and are able to be intercepted by anyone. They contain enough information and parameters for authorized users to gain access to the network. Regrettably, hackers can intercept the same information, and with special techniques to be discussed later, hackers can also gain access to the network. [27]

2. Rogue Access Points

As WLANs installations rapidly spread throughout the world, STAs and APs are made available in the marketplace with prices that are lowered almost every day. Users can purchase these devices and pay for them from their company’s petty cash, or from their own pockets in many instances. The users can connect those devices to their corporate network infrastructure without obtaining authorization from higher authorities in the company. There are also cases in which branches of companies and organizations installed Wireless Network components to their main corporate network infrastructure

without obtaining higher management and IT security authorizations. Wireless devices, especially APs, create immense network security risks for any company or organization. There is no real solution to this problem except monitoring the air for any new AP by using Wireless Network discovering tools such as NetStumbler. [27]

3. Unauthorized Use of Service

Since WEP is an optional protocol of the IEEE 802.11 standard, most of the wireless devices sold on the market today are sold with the service turned off as a default; and even when the service was turned on by the manufacturer, the devices have the same manufacturers' default keys used by all devices. This type of setup poses a potential risk to any WLAN because it is an open invitation for complete access by any hacker. To overcome this problem and to deter uninvited guests, WEP or any other security software tool must be turned on immediately, and all the default keys and values must be changed to the recommended length and values before going live on air. [27]

4. Service and Performance Limitations

WLANs have lower transmission capacity than traditional networks. Theoretically, the maximum speed of a Wireless LAN is about 54 Mbps (IEEE 802.11a) compared to up to 1 Gbps for traditional networks. The Wireless LAN capacity is shared between all STAs associated with an AP. It is very easy for a small or medium-sized WLAN to exhaust the throughput capacity when the network is busy. This makes it very easy for an attacker to launch a denial of service attack on the network from any rogue wireless station by overwhelmingly pinging the network's STA ports. Imagine the attacker launches his attack from a wired network at a rate much greater than the radio channel can handle. To minimize the risk of this type of attack, STAs and APs should be installed within close proximity with the signal strength set to a minimal strength just strong enough to cover the WLAN area. [27]

5. MAC Spoofing and Session Hijacking

Even though the IEEE 802.11 frames have a source address, there is no guarantee that the station sending the frame actually sent it on the air to the right destination. As mentioned earlier, the IEEE 802.11 standard does not authenticate frames and neither

does the standard protect the packets against a forged source address. The MAC addresses of participating wireless devices are sent in the open and can be intercepted by hackers who may utilize the information for malicious purposes. [27]

C. WIRED EQUIVALENT PRIVACY (WEP)

Since wireless transmissions are easier to intercept than transmissions over wired networks, and in order to bring the security level of Wireless Networks to a level closer to that of wired networks, the IEEE 802.11 committee not only specified the transmission protocols but also defined an optional protocol to address some of the security issues. Wired Equivalency Privacy (WEP) is the name given to such a protocol. It is implemented at the two lowest layers of the Open Systems Interconnect (OSI) reference model, data link and physical layers. The protocol is not intended to provide end-to-end security. The main goal of the WEP is to provide some kind of protection against the interception and alteration of data (integrity). Another goal of WEP is to provide access control to the WLAN infrastructure. The protocol was selected because it was thought to be reasonably strong, self-synchronizing and computationally efficient.

WEP uses Ron's Code4 Pseudo Random Number Generator (RC4 PRNG) algorithm. This algorithm is a symmetric key encryption algorithm developed by RSA Security Inc. The key stream in RC4 is independent of the plaintext, and encryption/decryption is done with reasonable speed. The algorithm also can be implemented easily in software. [28]

1. WEP Architecture

The RC4 PRNG algorithm uses an Integrity Check Vector (ICV) for every packet sent. The ICV is computed by performing a 32-bit cyclical redundancy check (CRC-32) on the frame. The computed ICV is then appended to the original frame to produce the plaintext. Afterwards, the RC4 PRNG algorithm uses a long sequence key stream to encrypt the plaintext message. The key stream is a function of the 40-bit secret key known by all APs and STAs and a 24-bit initialization vector (IV). To produce the final cipher-text, the plaintext is XOR-ed with the key stream and sent by radio to the destination.

To retrieve the original message at the receiving station, the same method explained above is performed but in reverse order. The receiver decrypts the cipher-text using a duplicated key stream to recover the plaintext and validates the checksum by computing the ICV and comparing it to the last 32 bits of the plaintext. Finally, it validates the checksum on the plaintext to ensure that only frames with a valid checksum are accepted. [28]

2. Attacks on the WEP

As mentioned above, the primary objective of WEP is to protect the confidentiality and integrity of data from unauthorized interception and modification. Disappointingly, with the weaknesses and vulnerabilities discovered by the researchers and network architects, WEP's security objectives can be defeated. The RC4 was found to contain major security flaws. These flaws allow a number of passive and active attacks that permit unauthorized interception and modification of data while it is being transmitted wirelessly from point to point. Some types of attacks on the WEP are discussed in the following section.

a. *Passive Attack to Decrypt Traffic*

The initialization vector (IV) is a 24-bit field used to randomize part of the key. All the combinations can run out within five hours for an IEEE 802.11b AP transmitting at 11Mbps according to Equation 1.

$$\frac{1500 \text{ bytes}}{\text{packet}} \times \frac{8 \text{ bits}}{1 \text{ byte}} \times \frac{1 \text{ sec}}{11 \text{ Mbits}} \times \frac{1 \text{ Mbit}}{10^6 \text{ bits}} \times 2^{24} \text{ packets} \approx 18,300 \text{ sec} \approx 5 \text{ hrs}$$

Time to exhaust 24-bit IV.

When the attacker collects two cipher-text packets encrypted with the same key, it is possible to perform statistical attacks to recover the plaintext. Afterwards, and when a cipher-text message with its plaintext version is definitely matched, an XOR operation can be performed which will reveal the key, and when the key is obtained, the hacker has everything. The equation takes the maximum packet size of 1500 bytes, and for a low traffic network, the time can increase dramatically. [28]

b. Active Attack to Insert Traffic

If the attacker knows the exact plaintext and its cipher-text, the key stream can be easily generated. After generating the key, the attacker can compile a message, and calculate its CRC-32 and XOR with the key to produce the cipher-text. Then, it can be sent to an Access Point or workstation as with any other legitimate traffic. [28]

c. Active Attack from Both Ends

If the attacker only knows the frame's header, which includes the destination and source IPs, it can be modified to change the source and destination IP to be his own as the source. When the AP receives the header along with the data, it transfers it to the destination address which is the source address of the hacker. When the destination station sends the reply, the new destination IP is that of the very happy hacker. [28]

d. Table-Based Attack (Dictionary Attack)

When the attacker figures out the plaintext of a packet, the key stream as mentioned above can then be computed. Therefore, the attacker can decrypt all the packets that are encrypted with the same IV and key stream. The attacker can collect all IVs and corresponding key stream in a table format "dictionary". This dictionary can contain up to 2^{24} , or more than 16 million, values, and each record is 1500 bytes. In brief, the dictionary size will be about 24 GB. If the attacker is able to build a dictionary of that size, any packet can be decrypted, regardless of the IV and key stream used. This is the ultimate goal of any attacker and the worst nightmare for any network security officer. [28]

3. Software Tools to Break the WEP

In order to intercept wireless data signals and gain control of a wireless network, several sniffing and capture tools and applications have been developed and made available free of charge to the public in the past three years. These sniffing tools are used to search for live WLANs. It is a very simple process and can be accomplished with several free tools run on mobile Pocket PCs such as MiniStumbler. Other hacking tools such as AirSnort, NetStumbler, Stumbler and Wellenreiter are used by hackers to break

into WLANs. These tools are built with sniffing and capture capabilities and are usually only available on Linux systems. One benefit to be said about these sniffing and capture tools is that they can be utilized by network administrators and IT Security Officers to troubleshoot and fix WLAN problems as well as evaluate the security level.

When the tools mentioned above go on air, they leave fingerprints in the form of unique text imbedded in their control, management and data frames. The information revealed by the fingerprints then can be used with Intrusion Detection System tools (IDS) to analyze data-link layer traffic. In the following section, a description is provided of how to detect each of the above-mentioned applications by analyzing their fingerprints.

4. Ethereal (Fingerprints Analyzer)

A protocol analyzer named Ethereal is used to examine captured data from a WLAN or any file. Each packet captured can be viewed and analyzed to find detailed information. The tool has many powerful features that allows filtering the search display by using a filter language. It can also reconstruct a stream of a TCP session and format it in a viewable screen.

In order to identify the fingerprint left by the sniffing tools, Ethereal version 0.9.5 is used as a tool for data collection using Libpcap version 0.7 libraries. A Cisco Aironet 352 card with Cisco Aironet version 1.8 drivers was also used for the experiment. The capture host ran Slackware 8.1 Linux and a custom 2.4.18 kernel. [29]

5. Using Ethereal to Discover Netstumbler

NetStumbler is used to detect a WLAN presence within a reasonable range and it displays the MAC address, the channel, the mode in which the WLAN is running and other information. It also can detect if any encryption is enabled. However, it cannot break any encryption if the encryption algorithm is enabled.

The tool uses active scanning through probe requests sent to a broadcast address with a broadcast Basic Service Set ID (BSSID) and an unspecified Extended Service Set ID (ESSID).

By using Ethereal, Mike Craik recognized a distinctive pattern that can be used to identify NetStumbler activities. Logical Link Control (LLC), which encapsulates frames

generated by NetStumbler, will use an organizationally unique identifier (OID) of 0x00601d and protocol identifier (PID) of 0x0001. The NetStumbler version can be identified because NetStumbler uses a 58 bytes size data payload containing a unique string with the version number. The unique string found in the data payload is shown in Table 5.

NetStumbler Version	Payload String
3.2.0	Flurble gronk bloopit, bnip Frundletrune
3.2.3	All your 802.11b are belong to us
3.3.0	intentionally blank 1

Table 5. NetStumbler Fingerprints.

MiniStumbler is a miniature version of Netstumbler that runs on a Microsoft Pocket PC. Although the binary “ministumbler.exe” program contains the string “All your 802.11b are belong to us”, this version of NetStumbler does not demonstrate the same characteristics as its Win32 equivalent.

The Ethereal was also successfully used to detect other scanning and sniffing tools such as Dstumbler, Wellenreiter and Windows XP, which was the first Microsoft operating system to include built-in support for 802.11 wireless networking. ([Layer 2 Analyses of WLAN Discovery Applications for Intrusion Detection, Joshua Wright, GCIH, CCNA. [29]

D. IMPROVING THE IEEE 802.11 NETWORK SECURITY

As more LANs and WLANs are deployed throughout the United States and around the world, and as more weaknesses are discovered with security elements of these networks, and especially with the WEP, there was a need to improve the security algorithm and mechanisms of the IEEE 802.11 family standards in particular, and network security, in general. Some of the ongoing efforts to address and enhance the security elements of both the Wired and Wireless networks are discussed below.

1. WEP2

The WEP2 is an enhancement to the original WEP protocol and is still based on the RC4 cipher. It is backwards compatible with WEP and works with most hardware. The new protocol uses an enlarged IV value and 128-bit encryption. The Integrity Check system is the same as for WEP and static keys will remain in the model.

In spite of the fact that the RC4 keystream is longer for the WEP2, it is expected that the difficulty in capturing the WEP2 key will increase slightly and it will take a few more hours to collect the necessary data. The updated WEP has failed to prevent IV replay exploits and still permits IV key reuse. In brief, WEP2 has been broken as happened to the original WEP.

2. IEEE 802.1x (Port-Based Network Access Control)

The IEEE organization developed and approved an IEEE 802.1x standard in June 2001 as a result of WEP and WEP2 and the many problems that proved their inability to deter hackers from infiltrating WALN traffic and resources. The standard is designed to support all wired and Wireless Networks that follow the IEEE 802 Local and Metropolitan Area Networks Port-Based Network Access Control standards, including the IEEE 802.11 Wireless Networks. The new standard defines a mechanism for Port-based network access control, which utilizes the physical access characteristics of the IEEE 802 LAN structure in order to provide methods of authenticating all devices attached to LAN/WLAN ports. It prevents access to the specified port when the authentication fails. As it stands, 802.1x does not, in reality, do any kind of encryption. It is used to authenticate users and to provide a secure way to exchange keys that can be used for encryption.

In the port-based network access control mechanism, a LAN port applies one of two roles: authenticator or supplicant. In the role of authenticator, authentication enforced by a LAN port before access by users allowed the port services through that port. In the role of a supplicant, a LAN port requests access to the services that can be accessed through the authenticator's port. An authentication server checks the supplicant's identifications and credentials on behalf of the authenticator. The authentication server

then responds to the authenticator, signifying whether the supplicant is authorized or unauthorized to access the authenticator's services.

The authenticator's port-based network access control defines two logical access points to the LAN through one physical LAN port. The first logical access point, data exchange between the authenticator and other computers on the LAN, is allowed by the uncontrolled port, regardless of the computer's authorization state. The second logical access point, the controlled port, allows data exchange between an authenticated LAN user and the authenticator.

IEEE 802.1x uses standard security protocols, such as Remote Authentication Dial-In User Service (RADIUS), to provide centralized user identification, authentication, dynamic key management and accounting.

a. 802.1x Authentication

The client sends a request for authentication to the AP. The AP replies with a request that the client provide identification, and blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the AP can verify the client's identity using the authentication server. Then, the client sends a response containing the identity to the authentication server. The type of identification is not specified in the protocol, but rather left up to the vendors, so authentication could be of any form.

The authentication server receives the request and uses an appropriate authentication algorithm to verify the client's identity. If the user can be identified, an accept message is sent to the AP. Otherwise, a reject message is sent.

If the authentication server accepts the client, then the AP will transition the client's port to an authorized state and forward additional traffic. [30]

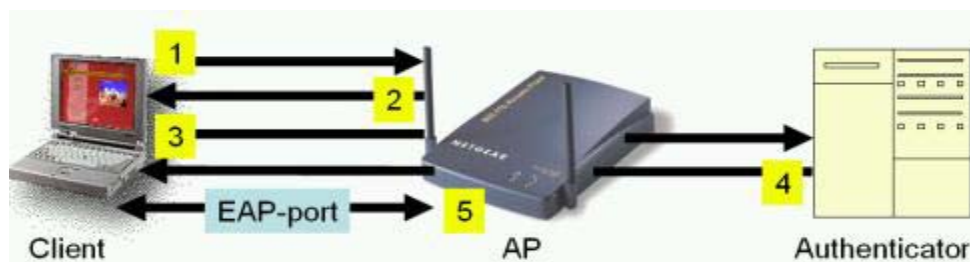


Figure 18. 802.1x Authentication Process, [From: 30].

b. 802.1x and Dynamic Key Management

As mentioned, the 802.1x standard provides authentication only. The standard does not denote the specific types of authentication or any type of encryption. However, as of June 2002, several vendors offer proprietary versions of dynamic key management using 802.1x as a delivery mechanism. Through dynamic key exchange, the authentication server can return session keys to the AP along with the accept message. The authentication server can return session keys to the AP along with the accept message.

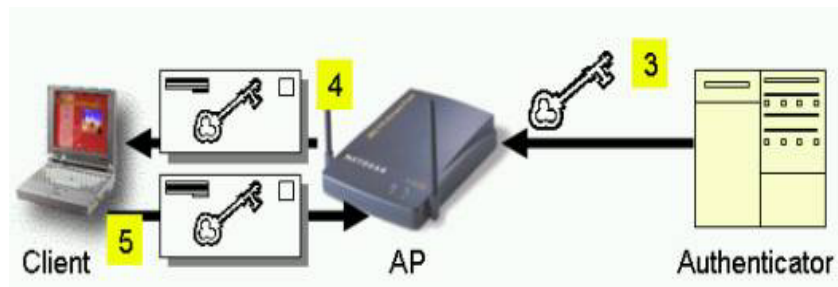


Figure 19. IEEE 802.1x Using Dynamic Session Keys [From: 30].

Instead of returning an accept message, the authenticator returns the results of the authentication and a session key if authenticated (step 3). The AP uses the session keys to sign and encrypt a message that is forwarded to the client after sending the success message (step 4). The client can then use contents of the key message to define proper encryption keys (step 5).

The connection using dynamic key management is more secure than manual management because it allows clients to automatically change the encryption key when they want and as often as they want to minimize any passive attack.

c. Problems with IEEE 802.1x

Unfortunately, the 802.1x protocol is not perfect. Cisco published “Cisco Security Advisory: Catalyst 5000 Series 802.1x Vulnerability” in April of 2001 regarding a problem with its own 802.1x implementation (Cisco, 2001). In addition, researchers at the University of Maryland found that 802.1x is prone to session hijacking and man-in-the-middle attacks.

In the session hijacking, the hacker waits for someone to authenticate successfully, and then sends a “disassociate” message to the workstation. The “disassociate” message looks as if it came from the original AP authorizing the connection (Spoofing). At this point, the user believes to be kicked off, but the AP thinks the user is still active. Next, and while the transmissions are not encrypted, the attacker can start using that connection up until the next time out (~1 hour). [30]

3. Internet Protocol Security (IPSec)

IP Sec is a set of protocols developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets at the IP layer. IPSec has been widely deployed to implement Virtual Private Networks (VPNs).

IPSec consists of Transport and Tunnel encryption modes. The Transport mode encrypts the payload part (data) of each packet and leaves the header in its original form. To elevate the Tunnel mode security, both the header and the payload are encrypted. At the other end, the receiving station decrypts each packet as it arrives or is queued before it is decrypted.

To successfully encrypt, send, receive and decrypt packets, the sending and receiving stations must share a public key, which is accomplished by implementing the Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley). The ISAKMP/Oakley allows the receiving station to obtain a public key and authenticate the sending station using digital certificates. As of today, there is no known case where the IPSec has been broken. [31]

E. WIRELESS NETWORK SECURITY RECOMMENDATIONS

As of today, strong wireless security mechanisms are very difficult to develop, test and implement because wireless network traffic is very easy to intercept, and therefore, easier to manipulate and analyze traffic, especially if there is no weak encryption algorithm employed for the data during interchange.

In order to minimize the risk of wireless network traffic interception and decryption, and to boost wireless network security, it is recommended that security be implemented in layers and stages. In addition, the following steps are recommended:

- The security algorithms and protocols such as the WEP must be enabled.
- The default SSID must be changed to a long and random sequence of characters that is difficult to guess.
- Dynamic sessions should be used along with MAC address filtering when possible if the product supports it.
- Consideration of using shared-key authentication rather than open authentication should be investigated.
- It is recommended to use products compatible with 802.1x or IPSec.
- Use of a Virtual Private Network (VPN) is a must for the military's wireless networks and any other high secret network.
- Establishing and tracking computer inventory is recommended to ensure accountability of all WNICs and block the MAC from any that are lost or stolen.
- Use of anti-virus and personal firewalls software is recommended to keep the wireless client clean.
- Placing all APs outside of firewalls to prevent any leak of traffic to the outside is important.
- Treating any point within the WLAN coverage (~300 feet) as a potential zone to deter hackers from intercepting the signals.

F. SUMMARY

In this chapter, wireless network security problems were discussed to show different attacks that are specific to wireless networks. The chapter also explained the techniques, algorithms and standards that were developed and are used to address most of these security problems. Finally, the chapter recommended steps and guidelines to elevate the security level of any wireless network and to minimize any adverse effect of a hacking.

The next chapter will research the market for required new wireless devices that are necessary to build an IEEE 802.11 wireless network. The chapter will also propose different designs for such networks to meet civilian and military requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

V. MARKET RESEARCH AND PRELIMINARY DESIGN

A. INTRODUCTION

In Chapter II of this thesis, wireless network components were introduced while Chapter III reviewed the IEEE 802.11 family of standards. In the previous chapter, wireless network security problems and vulnerabilities were discussed. In this chapter, market research will first be discussed describing available wireless network components that meet certain criteria.

Then using those selected devices, this chapter will formulate a broad design plan for wireless networks with different topologies and scenarios. It includes two topologies for wireless networks for civilian and military areas. The civilian wireless network design is presented as a speedy and cost effective broadband alternative solution for companies, organizations, institutions and home users in the Sultanate of Oman. The military wireless network design plan is also offered as an economical and speedy solution to the rapid deployment of military computer networks in the field of operations.

B. MARKET RESEARCH

As explained in Chapter II, the basic components of any wireless network are *Access Points (APs)* and *Wireless Network Interface Cards (WNICs)* which usually come as PCI or PCMCIA cards fitted in wireless *Stations (STAs)*. Furthermore, three more components are used to extend the coverage area of a wireless network: external antennas, WRs and amplifiers.

Since the approval of the IEEE 802.11 in 1997, many manufacturers started to launch devices compatible with that standard. In 1999, after the ratification of the IEEE 802.11b and due to its simplified design requirements, manufacturers began to ship devices compatible with the IEEE 802.11b ahead of the IEEE 802.11a. In mid 2002, the market received the long awaited IEEE 802.11a compatible devices. Moreover, in late 2002, due to the demand for backward device compatibility of IEEE 802.11a with the IEEE 802.11b networks, new APs, WNICs and *Wireless Routers (WR)* with dual frequency capabilities (2.4 and 5 GHz) were made available by many manufacturers.

Some of the new WNICs were compatible with the IEEE 802.1x and IEEE 802.11g (with added kit). Those new devices were made by Proxim Corporation, Netgear Incorporated, D-Link Systems, Cisco and other manufacturers.

The dual band devices examined during the market research can simultaneously operate in the 2.4 and 5.0 GHz and some of these devices promise to deliver data throughput up to 108 Mbps in the IEEE 802.11a mode and up to 22 Mbps in the IEEE 802.11b mode. It is concluded that the IEEE 802.11b devices can cover a three times larger area than the IEEE 802.11a devices. Therefore, the maximum data throughput for the IEEE 802.11a can be maintained when the distance is less than 60 feet indoors and about 400 feet outdoors whereas the distance is around 200 feet indoors and 600 feet outdoors for the IEEE 802.11b devices. It is noted through the market research process that the data throughput decreases as distance increases to the point where the signal significantly disperses and is no longer adequate to practically exchange data through the network.

The dual-band APs identified during the market research process were D-Link *AirPro* DWL-6000AP, Netgear WAB102, ORiNOCO AP-2000 from Proxim Corporation and Cisco Aironet 1200 Series APs. For the dual-band PCMCIA notebook cards, three were found: D-Link *AirPro* DWL-AB650, ORiNOCO 802.11a/b ComboCard and Netgear **WAG511 CardBus**. The only dual-band WNICs found for desktop PCs was D-Link *AirPro* DWL-AB520. However, many were found to be compatible with the IEEE 802.11a and IEEE 802.11b independently such as Netgear **HA311 802.11a**, Harmony 802.11a PCI Card from Proxim, ORiNOCO 802.11a PCI and others.

The market research revealed that there is a limited number of dual-band *Wireless Routers* (WR) available in the market to bridge WLANs with other WLANs/LANs. The only two dual-band WRs found are Linksys WRT51AB and D-Link *AirPro* DI-764.

As seen above, D-Link Systems offers a complete suite of wireless devices that are compatible with IEEE 802.11a, IEEE 802.11b and IEEE 802.1x. The devices are DWL-6000AP AP, a DWL-AB520 PCI card for desktop PCs and a DWL-AB650 PCMCIA adapter for notebook computers, and *AirPro* DI-764 *WR*.

In the following four subsections the technical specifications, operating modes and features of the mentioned D-Link devices in addition to the external antenna are discussed. The other devices mentioned above are very similar in their technical specifications, operations and features.

1. Access Point

The DWL-6000AP Multimode AP can connect to both 802.11a and 802.11b WLANs concurrently. The AP offers a total of eleven non-overlapping channels making it the ideal solution for any network administrator with the requirements of expanding the capacity of the WLAN. The non-overlapping channels allow users on different frequencies to connect to the network with minimal interference and collisions.

The DWL-6000AP offers transfer rates of up to 72Mbps in the 5GHz frequency range and up to 22Mbps in the 2.4 GHz frequency range which is considered to be above average data rates. The DWL-6000AP uses the latest advancements in the 802.11b silicon chip design from Texas Instruments, utilizing their patented *Digital Signal Processing* technology (DSP) combined with high-speed performance and features of the Atheros 802.11a chip design. The AP has also an integrated 10/100 Ethernet port to bridge it to wired networks. [32]



Figure 20. D-Link *AirPro* DWL-6000AP Access Point [From: 32].

In order for the DWL-6000AP to offer more secure communication, it features user-selectable encryption settings. These settings can be configured for the 5 GHz and

2.4 GHz modes separately. The WEP settings of the 5 GHz band can be configured up to 152 bits long and up to 256 bits long for the 2.4 GHz band. [32]

Device Management	<ul style="list-style-type: none"> • Web-Based – Internet Explorer v5 or later; Netscape Navigator v4 or later; or other Java-enabled browsers • Access Point Manager
Ports	(1) 10/100Base-T Ethernet, RJ-45 (UTP)
Standards	802.11, 802.11a, 802.11b, 802.1d, 802.3, 802.3u
Antenna Type	Dual 5dBi dipole antenna with diversity (standard)
Transmitter Output Power	15dBm ± 2dB
Power Input	External Power Supply — DC 5V, 2.5A
Certifications	FCC part 15b, UL1950-3
Data Rates	<p>802.11a Mode: up to 72 Mbps</p> <p>802.11b Mode: up to 22 Mbps</p>
Data Security	<p>802.11a Mode: 152-bit WEP, Access Control List</p> <p>802.11b Mode: 256-bit WEP, Access Control List</p>
Frequency Range	<p>802.11a Mode: 5.150 - 5.350 GHz</p> <p>802.11b Mode: 2.4 – 2.462 GHz</p>
Modulation Technology	<p>802.11a Mode: OFDM</p> <p>802.11b Mode: DSSS, PBCC - Packet Binary Convolutional Coding, 11-chip Barker sequence</p>

Table 6. DWL-6000AP AP Technical Specifications [From: 32].

2. Wireless Network Interface Cards (WNICs)

The DWL-AB520 is a WNIC for desktop computers and the DWL-AB650 is a wireless PCMCIA Type II CardBus for notebook computers, and both can connect to 802.11b or 802.11a WLANs at one time. The two cards are also compliant and interoperable with other IEEE 802.11a and 802.11b devices making them easier to connect to different devices from different manufacturers. The DWL-AB520 and DWL-AB650 are capable of achieving up to 54 Mbps data rates in the 5 GHz band and up to 22 Mbps in the 2.4 GHz band. In order to accomplish the best possible signal, the DWL-AB520 is equipped with a high-gain external antenna that can be positioned in any number of configurations. [32]



Figure 21. DWL-AB520 And DWL-AB650 [From: 32].

To achieve secure *Identification and Authentication* (IA), the two cards were made compliant with the IEEE 802.1x with dynamic keying. Furthermore, they also use the *Advanced Encryption Standard* (AES) with its 152-bit WEP for secure data transmission. [32]

Standards	IEEE 802.11a IEEE 802.11b IEEE 802.1x
OS Supported	Windows 98SE, Me, 2000, XP
Frequency Range	802.11a: 5.150 - 5.350GHz & 5.725 - 5.825GHz 802.11b: 2400 - 2.497GHz
Data Rates	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11b: 1, 2, 5.5, 11 Mbps
Encryption	Advanced Encryption Security (AES) 64/128/152-bit (Wired Equivalent Privacy) WEP
Antenna (DWL-AB520 only)	Omni-Directional Dipole Antenna with 2 ~ 4dBi
Transmit Power	802.11a - 13-14 dBm (54Mbps) 802.11b - 18 dBm (11Mbps)

Table 7. DWL-AB520 And DWL-AB650 Data Sheet [From: 32].

3. Wireless Router (WR)

A *Wireless Router* (WR) is similar to an AP with more capabilities and features. The primary goal of a wireless router is to connect WLANs together or WLANs with traditional wired networks. Wireless routers, unlike APs, provide *Network Address Translation* (NAT), *Dynamic Host Configuration Protocol* (DHCP), *Virtual Private Network* (VPN), roaming firewalls and more security elements.

The DI-764 is a wireless network router with multimode wireless broadband capabilities. The router can simultaneously bridge IEEE 802.11a and IEEE 802.11b WLANs with other WLANs. Additionally, with its four integrated 10/100 fast Ethernet ports, the router can expand the coverage area of WLAN to wider areas by bridging WLAN to traditional wired networks. Instead of using a dedicated traditional router, the DI-764 router enables administrators to easily set filters for the MAC address, IP address, URL and *Domain Name* (DN) and in order to elevate the network security, those filters can be set to be effective for a specific time of the day. [32]



Figure 22. DI-764 Wireless Router [From: 32].

The DI-764, like the DWL-6000AP, uses the high-speed Atheros 802.11a chip design combined with the Texas Instruments's latest 802.11b silicon chip. D-Link Systems has developed a very advanced web-based user friendly and easy to navigate management package to be used to set up the router easily and effectively. Finally, the DI-764 router can be used for multiple concurrent IPsec and PPTP VPN connections for mobile STAs to provide more security for sensitive data transmission. [32]

Device Management	<ul style="list-style-type: none"> • Web-Based – Internet Explorer v5 or later; Netscape Navigator v4 or later; or other Java-enabled browsers • Access Point Manager
Standards	802.11, 802.11a, 802.11b, 802.1d, 802.3, 802.3u
Available Channels	<ul style="list-style-type: none"> • (11) Non-overlapping channels (2.4GHz) • (8) Non-overlapping channels (5GHz)
Antenna Type	<ul style="list-style-type: none"> • 5dBi Dipole Antenna (5GHz) • 2dBi Dipole Antenna (2.4GHz)
Transmitter Output Power	15dBm \pm 2dB
Certifications	FCC part 15b, UL1950-3

Table 8. D-Link AirPro DI-764 Wireless Router Data Sheet [From: 32].

4. Antennas

The market research revealed that many antennas with different shapes and purposes are made for both IEEE 802.11a and IEEE 802.11b. It is found that *Telex Communications* offers a variety of antennas for internal and external use. The Omnidirectional antenna Telex 5830AA with 7.5 dBi gain () can cover up to three miles (4.75 km) from the AP/router when unhindered by hills, trees or buildings. Alternatively, several Telex 5840AA (15 dBi 90 degree panel) sector antennas can be installed to cover larger areas up to 6 miles (10 km). [19]



Figure 23. Telex 5830AN [From: 19].

Specifications	
Electrical:	
Frequency Range.....	5725 - 5825 MHz
VSWR.....	nominal 1.4:1, maximum 2:1
Nominal Impedance	50 ohms
Nominal Gain.....	7.5 dBi
Half-power Elevation Beamwidth	15 degrees
Polarization	Vertical
Maximum Power	10 watts
Mechanical:	
Size (without mount).....	1.0 OD x 10.875 inches
Mounting method	Bracket and SS clamp, 2.0 inch. OD mast max.
Connector	Type N jack
Wind Survival (per EIA-222-E at 100' height)	100 mph
Humidity	5% - 95% (non-condensing)

Table 9. Telex 5830AN Electrical and Mechanical Specifications [From: 19].

For the client’s outdoor antenna, Telex 5816AB Yagi antenna with 16.5 dBi gain is found to be the ideal solution due to its high gain and enclosed elements.



Figure 24. Telex 5816AB [From: 19].

Specifications	
Electrical:	
Frequency Range	5725-5825 MHz
VSWR	Less than 2:1, 1.5:1 Nominal
Nominal Impedance	50 ohms
Gain	16.5 dBi Nominal
Front-to-Back ratio	Greater than 20 dB
Half-power Beamwidth	19 degrees
Polarization	Vertical
Mechanical:	
Size	18.0" long
Mounting method	Clamps to vertical mast up to - 1 5/8" O.D.
Cable length	1.5 ft
Cable Type	LMR-195, 50 ohm
Connector	Type N jack
Optional connectors	TNC, TNC-RP, SMA, SMA-RP

Table 10. Telex 5816AB Electrical and Mechanical Specifications [From: 19].

To expand the coverage area, it is recommended that tower-mounted amplifiers with the antenna be used, and to mount them on heights above 100 feet in a flat area. This setup can provide a radio horizon of up to 14 miles in unobstructed plain areas. [19]

C. DESIGN PRINCIPLES

In addition to the general consideration of wireless networks deployment given in Chapter II, more considerations and steps are required to be taken in order to deploy large wireless networks. Tests such as end-to-end data throughput, reliability, interoperability with traditional networks, performance and other tests should be conducted by employing a thorough benchmark testing. Additionally, locations of the APs, routers, external antennas and amplifiers should be determined for each type of geographic location and for each category of application. [33]

As seen in the previous sections of this chapter, the technical specifications and features of the basic wireless network elements from different manufacturers have been briefly discussed and analyzed. More technical specifications and feature details were emphasized for the D-Link Systems equipment since D-Link Systems offers the full range of this equipment.

Additionally, Omnidirectional antenna Telex 5830AA with 7.5 dBi gain and a distance of up to three miles and the Telex 5840AA (15 dBi 90 degree panel) sector antennas with up to six miles (10 km) distance from *Telex Communications* were identified. As stated earlier, similar wireless devices and antennas with similar or better capabilities and features are also available from other manufacturers. Thus, when planning for wireless networks, more technical evaluations and testing should be conducted in order to determine the hidden and undocumented strengths and weaknesses of each type of device. [19]

In the following sections, two design plans for a civilian wireless network and a military wireless network are discussed to demonstrate how to build wireless networks for different applications using the aforementioned wireless network devices.

1. Design Plan for Oman Wireless Network

There are many different possible scenarios for the proposed wireless network design for Oman that could be utilized to implement wireless networks for different applications and environments in the country. Generally, the network can either be designed as a broadband service network for extending an existing wired network or as a completely wireless network with no connection to wired networks. The first topology is more practical for businesses, organizations, institutions and military formations that require connection to remote units and subunits with their existing wired networks. This design also can be used by *Wireless Internet Service Providers* (WISPs) to extend their services to home users who lack traditional Internet broadband access facilities. The second topology, completely wireless, is more practical when there is unavailability or unfeasibility of connection to the wired network for one reason or another.

One of the proposed wireless networks designs could consist of a main *Wireless Points Of Presence* (WPOP) equipped with necessary computer hardware, APs, WRs, Ethernet routers, high gain outdoor antennas and the necessary *Network Management Systems* software (NMS). The main WPOP will be connected to the existing wired network or to the outside world through Ethernet routers/gateways, satellite, microwave or fiber optics.

Additionally, the main WPOP may have one or more remote WPOPs, and each has at least one AP with an external directional antenna aimed at the main WPOP. All WPOPs will be connected with the main WPOP or with other WPOP either wirelessly, via WR/microwave, or via traditional Ethernet or fiber optics.

The WPOP could be mounted on the vast number of communications towers that already exist and positioned on the top of the mountains and along the major highways, cities and towns across the country. Fiber Optics, Ethernet bridges, WRs or microwaves could be used to achieve the connection between WPOPs and the wired network. When any of those connections are unavailable, satellite linkages are worth considering instead.

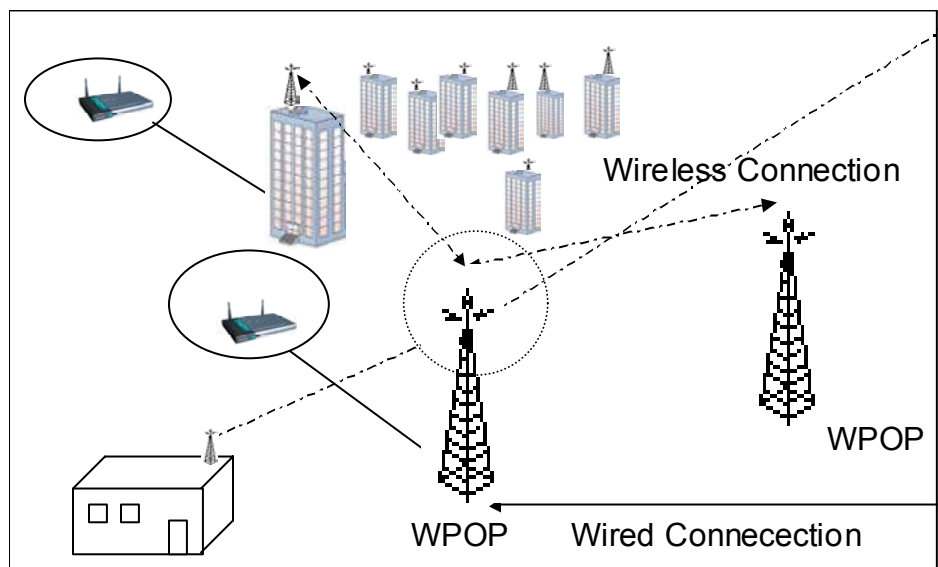


Figure 25. WPOP Representation.

Different possible scenarios are depicted in the figure below to accommodate different corporate clients and home users. Scenario 1 demonstrates a wireless network that is implemented within one building with one or more APs and without any connection to either a wired or wireless network. Scenario 2 depicts a wireless network connected to a wired network only, whereas scenario 3 demonstrates a wireless network with both wired and wireless network connections. Scenarios 4 and 5 illustrate wireless networks bridged together wirelessly and connected to the outside world through the WPOP, and finally, scenario 6 represents a home user with external antennas aimed at the nearest WPOP. The WPOP could be connected to a wired, wireless network or both.

There could be one or more APs and routers inside each building to cover all required offices. Those APs are also called Hotspots since they form some kind of surrounding electrical current in the form signals.

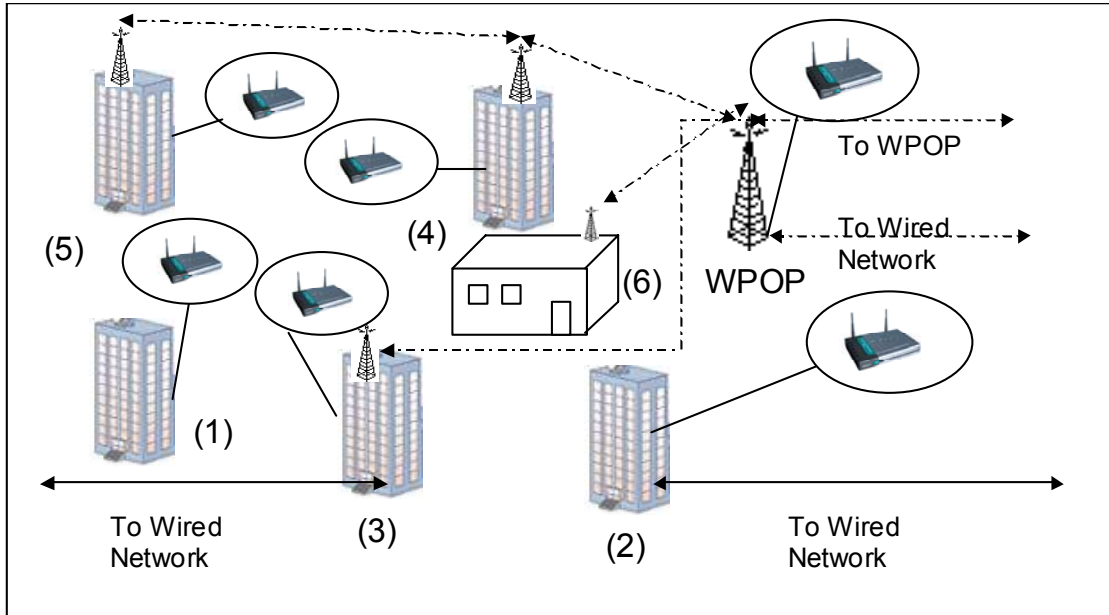


Figure 26. Different Wireless Network Scenarios.

Hotspots are installed in public places such as airports, public libraries, shopping malls and other public places. The connections to the Hotspots service can be offered free of charge or as a “pre-paid” service in the form a pre-paid password protected telephone like cards. This type of service will benefit people who travel frequently and stay away from their homes and offices. It also offers a practical way to utilize time while waiting for flights or traveling on trains close to Hotspots.

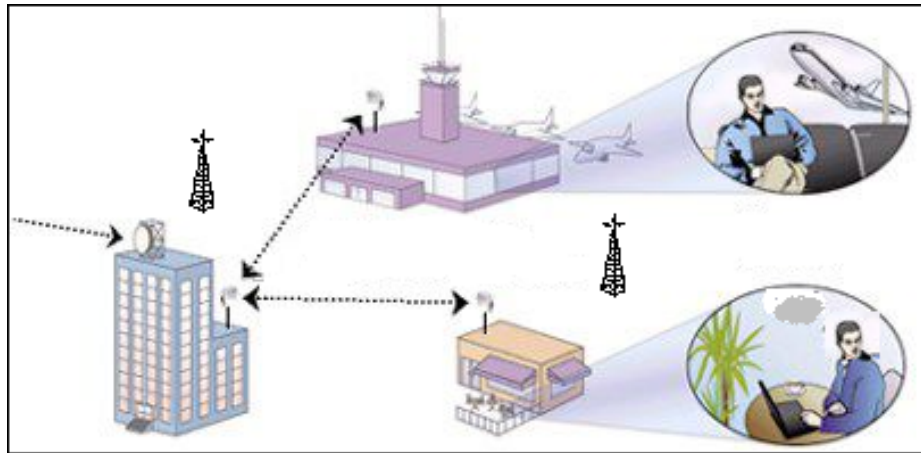


Figure 27. Wireless Public Access Points [After: 34].

To introduce *Wireless Internet Service (WIS)* in Oman, as a test pilot, it is suggested that the service first be gradually installed in Muscat City, the capitol, and its surrounding towns, which span more than 60 Km. The WPOPs could be installed on the existing communications towers and relay stations placed on the top of the mountains and hills around Muscat Town, Matrah, Ruwi, Alkhwair, Alqurum, Madinat A’ Sultan Qaboos and the Airport Heights. A proposed coverage area for the Muscat wireless network is depicted in the figure below.

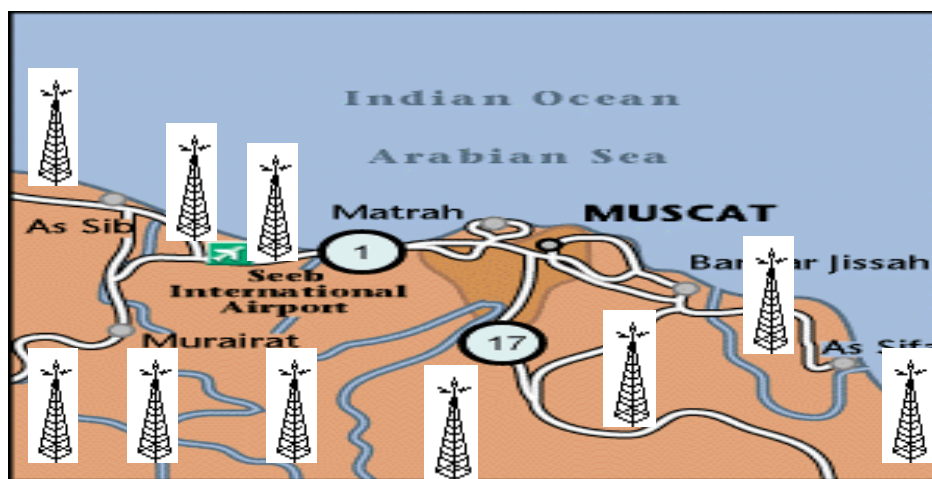


Figure 28. Muscat Wireless Network.

After a successful testing in Muscat, it is suggested that Hotspots to be installed in Salalah, Ibri, Suhar, Sur, Nizwa and other major cities and towns in Oman. Additionally,

wireless Hotspots are recommended for the Seeb International Airport, Salalah Airport, student dormitories at universities/colleges, major shopping centers, hotels such as the AlBustan Palace Hotel, Quorum National Park and Salalah plain in Dhofar which is a tropical leisure and camping area in the southern part of the country.

In order for a corporate, organization or institution to join and access the wireless network facilities, at least one WPOP with a directional external antenna aimed at the clearest and least crowded WPOP should be installed at the highest point possible. It is assumed that a site survey has already been established. Inside the buildings and offices, APs could be installed and can be added as required to cover more areas and relieve congested APs.

For home users, a desktop/laptop computer equipped with a WNIC with a directional external antenna, as needed, aimed at the clearest WPOP/Hotspot is required. If more computers are required to share the broadband service at home, an AP/WR should be installed. Additionally mobile and roaming users must be within range of at least one WPOP/Hotspot in order to be able to access the network.

Finally, it is assumed that any wireless network in the Sultanate of Oman is to be licensed and implemented under the Sultanate of Oman government rules and regulations, especially as regards the signal licensing issue. It is also recommended that the wireless network company will either be established as a joint venture with the existing national company or as a new competitive rival. In either case, access to the existing public telecommunication infrastructure under agreement between concerned bodies should be granted to the new company.

2. Military Wireless Network

There are a few suggested practical scenarios for the *Military Wireless Network* using the IEEE 802.11 standards. The first is a peacetime scenario where the main WPOP will be installed in the main static Headquarters camp, or any other stationary location, and will be connected to the military wired network via Ethernet, fiber optics or via WR. The other WPOPs will be installed in the remote static camps, bases, and naval ships and where required. The interconnections between land based static WPOPs can be achieved by the same methods discussed earlier; and the interconnection between WPOPs on the

naval ships, close to the coastline, and the land based static WPOPs can be achieved by WRs in the naval ships with external antennas pointed to the closest stationary land based WPOP. A fleet of nearby ships can utilize other ships WPOPs to form a float WWLAN.

In order to support mobile operations during wartime or exercise maneuvers, the main WPOP will be installed at the forward Headquarter or any other location in the field and will be connected to the rear main network by WRs, microwaves, satellites, fiber, Ethernet or high speed dialup modems. The other WPOPs will be deployed in the field brigades HQs, regiments, supply units and other units in the field.

Each group of clients in the field will have at least one Hotspot with an external antenna aimed at the nearest WPOP to form a WLAN. When more users are added to the network or when the data throughput decreases, more Hotspots can be added on the fly. In order to maximize the coverage areas of the field wireless network, more WRs are required to bridge two or more WPOP together.

In both peacetime and operation time, the military wireless network can be utilized by remote land stationary clients and naval ships close to the shores, to access the operational and administrative military systems such as the *Command and Control Systems* (CCS), *Human Resources Management Systems* (HRMS), *Logistics and Supply Systems* (LSS) and other military systems.

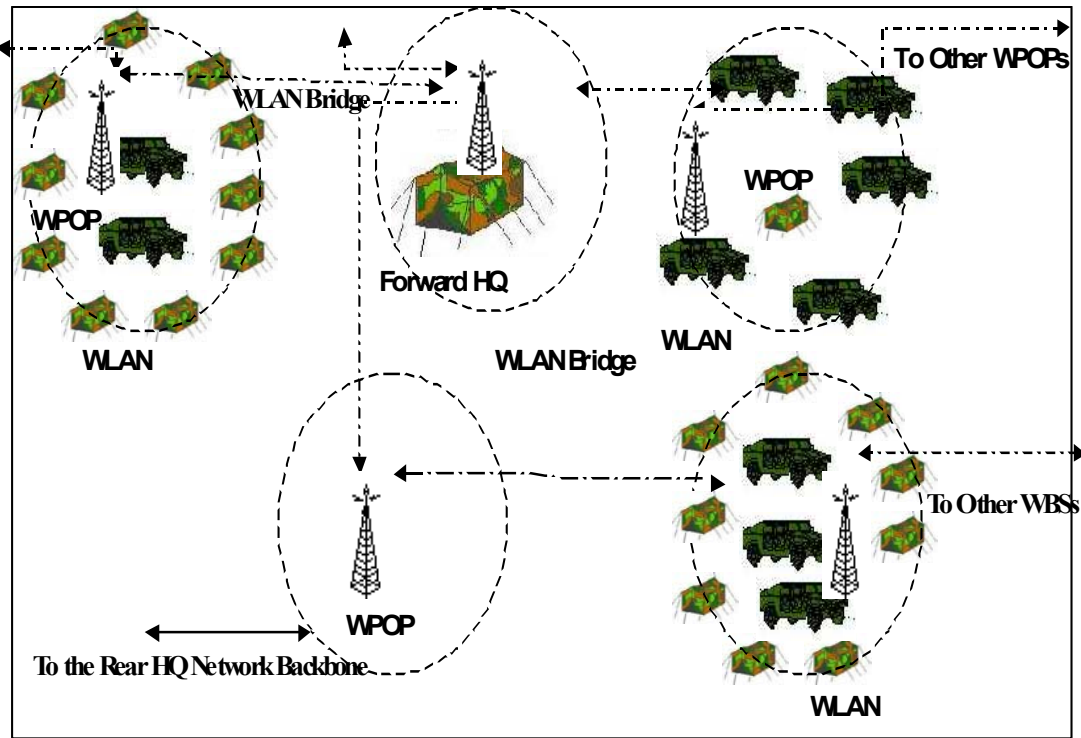


Figure 29. Military Wireless Network in the Field.

Due to the security nature of the military operations, using wireless networks in the military environment requires more considerations and planning. Additionally, all security protocols and features such as WEP and IEEE 802.1x must be turned on and set to the maximum allowable options. In order to maximize the security level, the use of IPSec and *Virtual Private Networks* (VPN) should be investigated when and where possible. These features must be checked and edited regularly to ascertain the compliancy of the security functions with the required assurance level.

There are companies, such as Harris Corporation of Melbourne, Florida, that are working to develop hardware and software to enhance the wireless network security and bring it close to the traditional wired network security. Recently, Harris Corporation has developed a *Secure Wireless Local Area Network* (SWLAN) interface card for government and military applications named SecNet 11. The card was tested and certified by the *National Security Agency* (NSA) as compliant with the *Type1 Encrypted Secure Wireless Networking* (ESWN) product.

3. A Broad Costing Plan

The market research has found that prices for all the wireless network devices from different manufacturers are very competitive since the market is flooded with such devices. The cost of the DWL-6000AP was found to \$200 and the price of the Netgear WAB102 \$215. Also, the prices of PCMCIA WNICs were found to be around \$100 and the prices for WRT51AB and DI-764WRs in the \$200 range.

In order to draft a cost plan, it is necessary to determine the number of required APs, WNICs, outdoor antennas, routers, amplifiers and other related equipment along with construction towers, cable, computer hardware and software for the providers and for the clients. Additionally, the digital circuit or any other connections charges and licensing, if required, should be included in the plan.

Table 11 shows the required wireless network devices and approximate cost of installing a 400 users wireless network in eight three-story buildings with a maximum distance of 3 Km between the two buildings. It is assumed that the connection between the wireless network and other wired/wireless networks already exists, and also, the required technical expertise and labor already in place. The same table can be used to estimate the cost of a military wireless network when installed in camps or in the field of operations with similar configurations and setup. The prices shown in the table are in Omani Rials (OR) with U.S. dollars in the last column. The Omani Rial is around 2.6 U.S. dollars.

	Units	Unit Cost	Total Cost (OR)	Total Cost U.S. Dollars
Servers with HW, SW and Accessories	9	1200	10800	28080
WNICs	420	40	16800	43680
APs	30	80	2400	6240
WRs	17	100	1700	4420
External Antennas	30	80	2400	6240
Grand Total			34100	88660

Table 11. Approximate Cost of Basic Wireless Network Devices.

D. SUMMARY

In this chapter, a market research was conducted to identify the available wireless devices in the market today that are compliant with the latest ratified IEEE 802.11 standards. The market research has resulted in identifying APs, WRs and WNICs compliant with the IEEE 802.11a, IEEE 802.11b and IEEE 802.1x. The chapter also proposed civil and military wireless network topologies and practical applications for those networks.

In the next chapter, a conclusion of the thesis will be provided to summarize the thesis topics and points of discussions and future work.

VI. CONCLUSIONS

A. SUMMARY

The thesis has introduced wireless network technology concepts, operations and benefits. It has described how wireless network were first started and how they have quickly developed to become one of the fastest growing technology sectors in the U.S. and around the world. The thesis described the different types of wireless networks including WPAN, WLAN, WWAN and WMAN.

The thesis has also introduced the IEEE 802.11 as the first internationally recognized standard for wireless networks including its history, architecture and services. It also described the DSSS, FHSS, HSDSSS and OFDM Physical layers and how they are used in the IEEE 802.11a and IEEE 802.11b. To complete the picture of the IEEE 802.11, the *Media Access Control* layer (MAC), its basic access method, different frames and formats were introduced to show how the MAC layer sends/receives the packets through the physical layer and how it acknowledges the sent frames. Other ongoing IEEE 802.11 tasks forces and workgroups were discussed briefly to show what new or updated standards can be expected soon, such as IEEE 802.11g, IEEE 802.11e and other draft standards.

The thesis has also examined the wireless network security problems and determined the vulnerability and security weaknesses that made wireless networks attractive to hackers. It also examined the available standards to support and enhance the security functionalities of wireless networks and measures to be taken in order to maximize the security level and minimize the adverse effects of an attack.

With the knowledge achieved through the study made in Chapters II through VI, market research was conducted in order to identity the available basic required wireless network devices that are compatible with the latest ratified IEEE 802.11 standards. The market research discovered that there are many reasonably priced devices from different manufacturers available in the market today which are compatible with those standards simultaneously in many cases.

Finally, the thesis has proposed a design plan for both a civilian and military wireless network. The civilian wireless network represented an Omani wireless network to fulfill the requirements for quickly deployable and cost effective broadband services in the country. The military wireless network presented a generic design plan for wireless network in the operation field that could be used by the military to meet the demands for a fast deployable and cost effective network during peacetime and operation time.

B. CURRENT TRENDS

According to the high-tech research firms, the number of WLAN chips sold in 2001 worldwide exceeded 8 million units and was expected to have reached more than 14 million chipsets in 2002. As the technology advances through the ratification of new standards, more and more organizations and companies are convinced to use them for their data and resources shares. Wireless networks are gaining momentum and becoming more widely used due to their proved reliability, scalability and mobility. The technology has also been proven to be effective and secure enough when certain guidelines and considerations are followed. Although the technology is still in its early stages of development compared to the wired networks, it has progressively developed and significantly matured due to the user demand for more enhancements that were met successfully by standard ratifications and device manufacturing.

Wireless networks have improved greatly since the approval of the IEEE 802.11 in 1997 and the sanction of IEEE 802.11a and IEEE 802.11b in 1999. Businesses and home users around the world have embraced wireless network technology since they provide all the functionality of wired LANs together with mobility, reasonable coverage and competitive data rates which has made them a big rival for wired networks. Wireless network technology also provides installation and configuration flexibility and eliminates or minimizes cabling requirements.

C. FUTURE WORK

It is expected that wireless network technologies will continue to develop and becomes more mature, efficient with better quality of service and more affordable. It is also expected that the data rates will increase steadily and become competent with wired

networks data throughput. The technology will become more secure to the level close to the wired networks by employing new techniques and algorithms.

These advancements in wireless network technologies will be made possible through the continuation of developments and ratifications of the wireless network standards such as the IEEE 802.11. The growth of the wireless networks deployments and usage will continue. Undoubtedly, the technology will play a major role in all facet of life including civilian and military areas and it will enter new fields that will change the existing businesses and organizations processes resulting in more services with mobility. One of the futuristic outlooks is the planned wide usage and proliferation of public and commercial Hotspots around the world. It is expected that the number of Hotspots here in the U.S. and Canada will reach 100,000 by 2007, and that in turn, will generate billions of dollars in service revenues. The newest venue for the wireless networks will be the commercial passenger planes. The idea is to equip Boeing 747-400 airliners and similar planes with high-speed WLAN by installing APs, routers and digital switches to provide Hotspots in the airplane or “Flying WLAN”. The connection to the outside world will be achieved by using satellite linkage providing real-time Internet access and data exchange services. Users can connect their notebooks to the plane’s WLAN and they can access the Internet while they are cruising the skies. The first experiment was carried here in the Silicon Valley last month.

It is the author’s intention to implement or assist in implementing some of the proposed wireless network scenarios during his future career and he believes that wireless network technology will benefit the entire country since it provides an easy, quick and less costly alternative to traditional networks. Moreover, due to the ever-evolving wireless network technology and the many advantages and savings expected from implementing such technology, it is the author’s objectives and expectations to continue his study and research of the wireless network technologies when the circumstances permit.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- [1]. [http://www.hp.com/sbso/productivity/howto/wireless_2.html], February 2003.
- [2]. Wireless Local Area Networking: An Introduction, [<http://www6.tomshardware.com/network/01q3/010822>], March 2003.
- [3]. Standards Based Wireless Networking with Linux, [<http://www.linux-wlan.com/writings/std-wlan-linux/stdwlan-whitepaper.html>], March 2003.
- [4]. Introduction Wireless LAN, [<http://www.sss-mag.com/pdf/wlanintro.pdf>], March 2003.
- [5]. Standards Based Wireless Networking with Linux, [http://www.aksa-sds.com/PdfFiles/white_paper_wpan.pdf], March 2003.
- [6]. Local Area Network, [http://isp.webopedia.com/TERM/L/local_area_network_LAN.html], March 2003.
- [7]. Feature - Wireless Wide Area Networks, [http://www.pdafn.com/vertical/features/wireless_4.xml], March 2003.
- [8]. IEEE 802.16 for Broadband Wireless, [<http://www.nwfusion.com/news/tech/2001/0903tech.html>], March 2003.
- [9]. IEEE Standard 802.16: A Technical Overview of the Wireless MAN Air Interface for Broadband Wireless Access, [http://grouper.ieee.org/groups/802/16/docs/02/C80216-02_05.pdf], March 2003.
- [10]. The Wireless Internet in North America, [http://www.airprime.com/CDMA_White_Paper.PDF], March 2003.
- [11]. The Wireless Internet in North America Agency Reduces Power on 72-Mile WLAN Link, [<http://www.computerworld.com/mobiletopics/mobile/story/0,10801,76118,00.html>], March 2003.
- [12]. Wireless Service Providers Plan to Spend \$1.1 Billion, [<http://www.wispa.org>], March 2003.
- [13]. Wireless Networking: Overview and Roadmap, [http://www.ieee.or.com/Archive/80211/IEEE_Blyler.pdf], March 2003.
- [14]. Access Points, [http://www.intel.com/network/connectivity/solutions/wireless/tech_access.htm], February 2003.

- [15]. Access Points, [http://www.linksys.com/splash/wap54g_splash.asp], March 2003.
- [16]. Netgear, [<http://www.netgear.com/>], March 2003.
- [17]. International Engineering Consortium, [<http://www.iec.org/cgi-bin/acrobat.pl?filecode=128>], March 2003.
- [18]. Proxim Wireless Networks, [<http://www.proxim.com/products/all/orinoco/client/index.html>], March 2003.
- [19]. Telex, [<http://www.telexwireless.com/index.htm>], March 2003.
- [20]. Cisco Systems, [<http://www.cisco.com/univercd/cc/td/doc/product/wireless/bbfbw/ptop/p2pspg02/spg02ch2.htm>], March 2003.
- [21]. Wireless Tek, [<http://www.wirelesstek.com/>], March 2003.
- [22]. WLANA, [<http://www.wlana.org/learn/health.htm>], February 2003.
- [23]. Bob O'Hara and Al Petrick, IEEE 802.11 Handbook: A Designer's Companion, IEEE Press, 1999.
- [24]. ANSI/IEEE Std 802.11, 1999 Edition, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
- [25]. [<http://britneyspears.ac/physics/intro/hedy.htm>], March 2003.
- [26]. Understanding 802.11 Frame Types, [<http://www.80211-planet.com/tutorials/article.php/1447501>], March 2003.
- [27]. Seven Security Problems of 802.11 Wireless, [<http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html>], March 2003.
- [28]. Wired Equivalent Privacy Vulnerability, SANS Institute, [<http://rr.sans.org/wireless/equiv.php>], March 2003.
- [29]. Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection, [<http://home.jwu.edu/jwright/papers/l2-wlan-ids.pdf>], March 2003.
- [30]. SANS Institute, 802.11, 802.1x, and Wireless Security, J. Philip Craiger, June 23, 2002, [<http://www.sans.org/rr/wireless/80211.php>], March 2003.
- [31]. IPsec, [<http://www.baltimore.com/devzone/standards/ipsec.asp>], March 2003.
- [32]. D-Link, [<http://www.d-link.com/>], March 2003.
- [33]. National Science Foundation, [<http://wireless.oldcolo.com/course/method.htm>], March 2003.

- [34]. Public Hotspots,
[\[http://www.proxim.com/products/serviceprovider/solutions/publicaccess.html\]](http://www.proxim.com/products/serviceprovider/solutions/publicaccess.html),
March 2003.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

802.11 Standard, [http://cepheus.nat.sdu.dk/wlan/802_11standard.htm], March 2003.

Defining a Wireless Solution, [<http://www.developer.com/ws/other/article.php/1482501>], March 2003.

G. M. Lundy, M. Almquist and T. Oruk, “Specification, Verification and a Simulation of a Wireless LAN Protocol: MACAW.

Lufthansa and Cisco Put Wi-Fi in the Plane, [<http://www.80211-planet.com/news/article.php/1570531>], March 2003.

Oman Telecommunications Company, [<http://www.omantel.net.om>], March 2003.

Our Wireless Future: An IBM Vision, [<http://www.eaijournal.com/BIJ/PDF/OurWirelessFuture.pdf>], March 2003.

Wireless Communications and Networks, William Stallings, Prentice Hall, 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Major General. Ahmed Alnabhani
Commander Royal Army of Oman
P.O. Box. 721
Muscat, 111
Sultanate of Oman
4. Staff Brigadier. Saif Almaani
Ministry Of Defense
P.O. Box 113
Muscat, 113
Sultanate of Oman
5. Prof. Gilbert Lundy
Naval Postgraduate School
1 University Circle
Monterey, CA
6. Prof. Riehle, Richard
Naval Postgraduate School
1 University Circle
Monterey, CA
7. Monther Almanthery
P.O. Box. 1355
Muscat, 111
Sultanate of Oman
8. Ahemd Almanthery
P.O. Box. 1355
Muscat, 111
Sultanate of Oman