



NEAR EAST UNIVERSITY

GRADUATE SCHOOL OF APPLIED AND SOCIAL
SCIENCES

SECURING AND MANAGING WIRELESS
NETWORKS

Examining Committee in charge:

Atif Munir

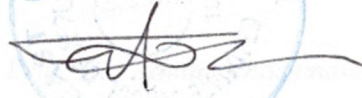
Master Thesis

Department of Electrical and Electronic
Engineering

Nicosia - 2005

Approval of the Graduate School of Applied and
Social Sciences

Prof. Dr. Fahreddin M. Sadiko lu
Director



We certify this thesis is satisfactory for the award of the
Degree of Master of Science in Electrical and Electronic
Engineering

Examining Committee in charge:

Assoc. Prof. **Dr. Adnan Khashman,**

.C>:

Committee Chairman,
Chairman of Electrical and
Electronic Engineering
Department, NEU

Assist. Prof. Dr. brahim Arkut,

918-t.t,/t-

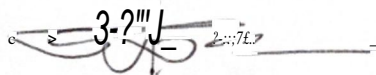
Member, Computer
Engineering Department, NEU

Dr. Erkut inan i eri,

G.t.-1-/-~

Member, Electrical and
Electronic Engineering
Department, NEU

Prof. Dr. Fahreddin M. Sadiko lu,



Dean of Engineering Faculty,
Supervisor, NEU

ACKNOWLEDGEMENTS

First of all, I would like to avail this opportunity to thank Prof Dr. Fakhraddin Mamedov for supervising me in my thesis, and being there when it mattered most in almost all of my educational requirements, and Prof Dr. Senol Bektas, for holding my hands and giving me the light of hope. Without their help I would have never made it to this level, ever.

Then I would like to thank, Assoc. Prof Dr. Adnan Khashman, and my colleagues in the University, especially Jamal, for being kind to me and being very direct in their approach.

And Mr. izzet Agoren and Ayza Net. This thesis is indebted to their kindness and willingness. Thank you, for believing in me.

And last, God All Mighty and my family, for backing me up no matter what the circumstances had been. They have been there when ever I felt the burden.

Thank You

Atif Munir

ABSTRACT

Over the last ten years, cell phones, pagers, and wireless Personal Digital Assistants (PDA) have become so commonplace in our lives that it is easy to forget those ten years ago, they were a rarity. But wireless communications is still in its infancy, and the next stage of its development will be in supplementing or replacing the network infrastructure that was traditionally "wired" as well as enabling network infrastructures that previously could only be imagined. And with this challenge, comes the problem of developing such means and measures that would make a wireless LAN network secure and breach free.

Development of new software such as Netstumbler and AirSnort along with smart and causal antennas has made the existing wireless networks increasingly insecure and easy to compromise. Disabling Extended Service Set Identifier (ESSID), giving static IP (Internet Protocol) addresses to customers, Wired Equivalent Privacy (WEP) encryption and above all, even Media Access Control (MAC) Address Filtering cannot help but make our lives increasingly stressful.

This Thesis presents a better way of securing a wireless network by introducing a Certificate Authority authentication mechanism with Protected Extensible Authentication Protocol (PEAP) for issuing encrypted certificates not only to the clients but also to the access points in the network itself, hence minimizing the attack level on the whole wireless network. Further more, algorithms will be developed to enhance the Microsoft Internet Security Server (ISA 2004) for the protection of the network from both internal and external threats.

This thesis will also present some 2.4 GHz antenna prototypes which will be tested with a reference industrially manufactured antenna and hence concluded for feasibility and strength.

TABLE OF CONTENTS

ACKNOWLEDGEMENT	i
ABSTRACT	ii
TABLE OF CONTENTS	iii
LIST OF ABBREVIATIONS	vii
INTRODUCTION	x
1. INTRODUCTION TO WIRELESS NETWORKS	1
1.1 Overview	1
1.2 Difference between a wired and a wireless network	1
1.3 Wireless terminology and evolution	3
1.3.1 Broadband	3
1.3.2 Wide area network	3
1.3.3 Brief History of wireless licensing	4
1.4 License free Wireless Frequencies	6
1.5 Advantages of License free wireless networks	6
1.6 Challenges of License free wireless networks	7
1.7 Exploring present applications for Wireless	7
1.7.1 Applying Wireless Technology to vertical markets	9
1.7.2 Applying Wireless technology to Horizontal applications	11
1.8 Basic Elements of a Wireless Network	12
1.9 Basic Antennas and Types	16
1.9.1 Omnidirectional Antennas	16
1.9.2 Directional Antennas	18
1.10 BiQuad Antenna	23
1.10.1 Construction Of BiQuad Antennas	24
1.10.2 Comparisons and Testing	32
1.10.3 Conclusions	39

1.11 Summary	40
2. THE INTERNET PROTOCOL IN A WIRELESS NETWORK	41
2.1 Overview	41
2.2 Introduction to Internet Protocol	41
2.3 IP Addressing	43
2.4 Conserving Address space with VLSM	46
2.5 IP Routing	48
2.6 Internet Control Message Protocol	50
2.7 Understanding the Host to Host layer	51
2.8 Managing Application Layer	55
2.9 Summary	59
3. FIXED WIRELESS TECHNOLOGIES AND STANDARDS	60
3.1 Overview	60
3.2 Multichannel Multipoint Distribution Service	60
3.3 local Multipoint Distribution Service	62
3.4 Wireless Local Loop	63
3.5 Point-to-Point Microwave	65
3.6 Wireless Local Area Networks	67
3.7 Need for a Wireless LAN Standard	67
3.7.1 Definition of WLAN standards	68
3.7.2 Guaranteeing compatibility	69
3.8 802.11 a Standard	72
3.9 Developing WLANs through 802.11 Architecture	74
3.9.1 The Basic Service Set	74
3.9.2 The Extended Service Set	76
3.10 Services to the 802.11 Architecture	77
3.11 The CSMA-CA Mechanism	80

3.12 The RTS/CTS Mechanism	80
3.13 Summary	81
4. AUTHENTICATION OF A WIRELESS NETWORK IN WINDOWS ENVIRONMENT	82
4.1 Overview	82
4.2 Overview of Network Configuration	82
4.3 Protected Extensible Authentication Protocol (PEAP)	85
4.4 Installing and configuring a Certificate Authority	89
4.4.1 Installing Certificate Services	89
4.4.2 Installing a Certificate on a RADIUS server	91
4.5 Installing and configuring a RADIUS server	92
4.5.1 IAS Installation	93
4.5.2 IAS Configuration	93
4.6 Configuring AD users and the RADIUS policies for access	96
4.7 Microsoft Internet Security and Acceleration Server 2004	96
4.7.1 Installing and Configuring ISA server 2004	97
4.7.2 Checking for Internet Connectivity	100
4.7.3 Configuring the ISA rules for the Desired Access Levels	102
4.8 Configuring Wireless Access Points	105
4.8.1 Configuring a Link.sysAccess Point	105
4.8.2 Configuring a D-Link Access Point	110
4.9 Configuring Wireless setting in XP	113
4.10 Comparison and Conclusion	115
4.11 Summary	120
5. CONCLUSION	121
6. REFERENCES	123

APPENDIX - I -	127
APPENDIX - II -	129
APPENDIX - III -	134
WAN	Wide Area Network
MAN	Metropolitan Area Network
LAN	Local Area Network
FTD	Federal Communications Commission
ISDN	Integrated Services Digital Network
WSPS	Wireless Personal Service Provider
VPN	Virtual Private Network
PDN	Personal Data Network
SPN	Specialized Service Network
UPS	Unified Parcel Service
GPS	Global Positioning System
WAP	Wireless Application Protocol
SMG	Short Message Service
PC	Personal Computer
FM	Frequency Modulation
AM	Amplitude Modulation
PCB	Printed Circuit Board
SNR	Signal to Noise Ratio
dBm	Isotropic Decibel Power
dBW	Decibel Power per Meter
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLSM	Variable Length Subnet Mask
ICMP	Internet Control Message Protocol
SNMP	Simple Network Management Protocol
DHCP	Dynamic Host Configuration Protocol

LIST OF ABBREVIATIONS

L.A.	Local Area Network
W.A.	Wide Area Network
MAN	Metropolitan Area Network
WiLAN	Wireless Local Area Network
FCC	Federal Communications Commission
ISM	Industrial Scientific and Medical
WISPS	Wireless Internet Service Providers
VPN	Virtual Private Network
PDA	Personal Data Assistant
ESMR	Enhanced Specialized Mobile Radio
Ups	United Parcel Service
GPS	Global Positioning System
WAP	Wireless Application Protocol
SMS	Short Message Service
PC	Personal Computer
FM	Frequency Modulation
AM	Amplitude Modulation
Pcb	Printed Circuit Board
SNR	Signal to Noise Ratio
dBi	Isotropic Decibel Power
dBm	Decibel Power per Meter
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLSM	Variable Length Subnet Mask
ICMP	Internet Control Message Protocol
SNMP	Simple Network Management Protocol
DHCP	Dynamic Host Configuration Protocol

MAC	Media Access Control
NAT	Network Address translation
PAT	Port Address Translation
OSI	Open System Interconnectivity
MMDS	Multichannel Multipoint Distribution Service
DSL	Digital Subscriber Line
RPC	Radio Port Controller
LMDS	Local Multipoint Distribution Service
WLL	Wireless Local Loop
POTS	Plain Old Telephone Service
LE	Local Exchange
FAU	Fixed Access Unit
RP	Radio Port
PTP	Point-to-Point Microwave
IEEE	Institute of Electrical and Electronic Engineer
PHY	Physical Layer
IR	Infrared
FHSS	Frequency Hopped Spread Spectrum
DSSS	Direct Sequence Spread Spectrum
WECA	Wireless Ethernet Compatibility Alliance
U-NII	Unlicensed National Information Infrastructure Spectrum
OFDM	Orthogonal Frequency Division Multiplexing
QoS	Quality of Service
DS	Distribution Service
BSS	Basic Service Set
ESS	Extended Service Set
WEP	Wired Equivalent Protocol
AP	Access Point
LLC	Logical Link Control
CSMA-CA	Carrier Sense Multiple Access Collision Avoidance

CSMA-CD	Carrier Sense Multiple Access Collision Detect
RTS/CTS	Request To Send/Clear To Send
PEAP	Protected Extensible Authentication Protocol
ISA	Microsoft Internet Security and Acceleration Server
DMZ	Demilitarized Zone
WPA	Wi-fi Protected Access
RADnJS	Remote Authentication Dial In User Service
EAP	Extensible Authentication protocol
TLS	Transport Layer Security
SSL	Secure Server Layer
PKI	Public Key Infrastructure
LEAP	Light Extensible Authentication Protocol
IS	Internet Information Services
IAS	Internet Authentication Service
IT	Information Technology
DNS	Domain Name Service
AES	Advanced Encryption Standard

INTRODUCTION

Wireless access to corporate resources while in the office, at home or while traveling is now a reality and offers a very flexible approach to networking. Along with the introduction of wireless local area networks (WLANS) comes the unique security issue that needs to be addressed when clients access an open wireless network.

The Objective of this thesis is to present a better security mechanism by introducing a Certificate Authority server in the network for authentication of the clients in the network as well as the access points in the network, hence giving the users end to end authentication from a mobile unit all the way to the internal servers.

This thesis will also present some 2.4 GHz antennas developed by the author and they will be tested and compared with an industrially manufactured antenna for feasibility and strength.

In chapter 1, the basics of wireless networks, the terms involved in broadband technology and both challenges involved and advantages of deploying a license-free wireless technology will be discussed. Further more, the basic wireless elements and some wireless antennas will be taken into consideration along with some antenna prototypes developed by the author, which will be tested and compared with an industrially manufactured antenna.

When designing and implementing networks today, it is important to have a good understanding of the network layer protocol that will run over them. In chapter 2, the properties of the TCP/IP protocol will be studied. This chapter will cover both the OSI model and the TCP/IP protocol suite, identifying specific examples and correlations to wireless networking.

Chapter 3 identifies some of the many wireless-networking technologies. This chapter will present the various forms of new wireless topologies to enhance a wireless network along with the new emerging standards.

In chapter 4, a secure wireless network is developed using Protected Extensible Authentication Protocol (PEAP) and Microsoft Internet Security and Acceleration (ISA) Server 2004. A Certificate Authority will be implemented to issue certificates for authenticating the clients as well as the access points. Some prototypes of Wireless Access points will be configured accordingly. The Network will be tested and compared with another network without these security measures and results are shown.

In the conclusion, the author shows the implementation of such a network along with all the necessary protocols and methodologies involved.

Most of the time, the term of wireless network is not understood as a network between using a wireless network and using a wired network. The difference between a wired network and a wireless network is designed in completely different in comparison to monitoring and managing a wired network. The table 1.1 below describes some of the main differences.

Table 1.1 Main differences between a wired and a wireless network

Parameter	Wired Network	Wireless Network
Installation	If the network cable is going to the location, the location can be connected to the network.	Wireless networks are direct connect to location and cannot be connected to the network. Additionally, wireless network might not be visible area.

1. INTRODUCTION TO WIRELESS NETWORKS

1.1 OVERVIEW

In this chapter, the basics of wireless networks, the terms involved in broadband technology and both challenges involved and advantages of deploying a license-free wireless technology will be discussed. Further more, the basic wireless elements and some wireless antennas will be taken into consideration along with some antenna prototypes developed by the author, which will be tested and compared with an industrially manufactured antenna.

1.2 DIFFERENCES BETWEEN A WIRED AND A WIRELESS NETWORK

Most of the time, the users of broadband wireless network do not experience a difference between using a wireless network and using a wired network. The experience as a wireless network is designed is completely different as compared to installing and deploying a wired network. The table I. I below describes some of the main differences.

Table 1.1 Main differences between a wired and a wireless network

Network Characteristics	Wired Network	Wireless Network
Visual determination of network connectivity.	If the network cable is seen going to the location, that location can be connected to the network.	Wireless networks sometimes connect to locations that cannot be visibly seen. Additionally, wireless networks might not Connect locations that can be visibly seen.

Visibility node-to-node on the same network.	All of the nodes of a wired network can hear all other nodes.	Many nodes of the wireless network cannot hear all of the other wireless nodes on the same network.
Visibility network-to-network	Wired networks are invisible to other wired networks: The presence of one wired network has no effect on the performance of another wired network	Wireless networks are often visible to other wireless networks. One wireless network can affect the performance of other wireless network.
Atmospheric Properties	Wired network performance is not affected by the properties of the atmospheric properties.	Wireless network performance can be affected by the properties of the atmosphere.
Terrain Properties	Wired network performance is not affected by the properties of the earth's terrain.	Wireless network performance can be affected by the properties of the earth's terrain.
User connectivity and mobility.	Connectivity is possible only to or from those physical locations where the network cabling extends.	Connectivity is possible beyond the bounds of the physical network cabling.

1.3 WIRELESS TECHNOLOGY AND EVOLUTION

Today, engineers are capable of designing and maintaining a wireless network that has three major characteristics that were not available in the past. These characteristics are broadband capability, Wide Area coverage and license-free operation. The definition of these terms are somewhat vague, therefore it's necessary to define these terms appropriately.

1.3.1 Broadband

Broadband is a subjective term that can be used in various ways throughout the communications industry. Broadband is used when new communication technologies are developed that provide enough additional bandwidth for the user experience to feel substantially faster than it felt before.

Most internet users today have experienced dialing into the Internet at bandwidths ranging from 28,800 bits per sec (28.8 kbps) up to 56,000 bits per sec (56 kbps). They perceive a faster internet connection, such as 1.5 million bits per sec (1.5 Mbps) connection, as a broadband connection. Some users have access to the Internet using a web browser on a cell phone. Their connection bandwidth ranges from 9.6 kbps to 14.4 kbps. Comparing the cell phone connection to that of a dial-up, the cell phone connection feels slow. It is thus termed as a 'narrow band' instead of a broad band. It is usually acquired that any speed of 128 kbps or higher is termed as a 'Broadband connection'.

1.3.2 Wide Area Network

There's no absolute line between the definition of a local-area network (LAN) and the definition of a Wide-area network (WAN). Both these terms have been used somewhat loosely. But wirelessly, they could be defined in these two categories as:

- LAN- A network that connects stations contained within a single building.
- WAN- A network that connects stations located in different buildings or in different parts of the city.
- MAN- A network which indicate a metropolitan-area network, or in other words, a citywide network.

1.3.3 Brief history of wireless licensing

Wireless technology has passed through several regulatory phases during its history. In the early days, transmitting distances were limited and population density was low: it was unnecessary to require a license for transmitting. As more wireless stations came on the air, interference between stations became a serious problem. So, the governments began requiring licenses for all transmitters, including commercial broadcasts transmitters, experimental transmitters, and amateur radio transmitters.

Radio system usage continued to grow more rapidly during the remainder of the 20th century. The radio transmissions and radio transmitters continued to get licensed. These licensing regulations played a useful role because they allowed many different radio systems to share the available radio frequencies without interfering with each other.

The downside to government regulation was that it took both time and money to obtain a license to transmit on a specific frequency. This limited the use of broadband wireless equipment to those companies or individuals who could afford the cost of obtaining the license and purchasing the rather expensive wireless equipment.

In 1985, the Federal Communications Commissions (FCC) issued regulations that for the first time, allowed the use of the broadband wireless transmitting equipment

without the need to apply for, pay for, and wait for a license [1]. To operate license free, the wireless equipment had to do the following:

- Operate at low power levels
- Use spread spectrum modulation
- Transmit within three specified frequency bands

Broadband license-free wireless equipment began to be manufactured and sold at a much lower cost than the licensed broadband wireless equipment.

Prior to the regulations, FCC permitted low power, short range devices such as baby monitors or garage door openers to operate license free. These devices operated indoors or with short range transmitters and did not cause interference problems with other wireless systems. Then however, the following points were considered and then it was decided to allow the operation of license-free spread spectrum systems:

- Spread spectrum signals spread their wireless energy over the frequency spectrum rather than concentrating all on one frequency. By spreading out the energy, the signals are less likely to cause interference to other spread spectrum and non-spread spectrum systems.
- Spread spectrum signals are less susceptible to being interfered with than non-spread spectrum signals.

- Low power spectrum transmitters operating in the ISM (Industrial, Scientific and Medical) bands will be limited to the line-of-sight operation. The signals will not carry very far; therefore many spread spectrum systems can operate in the same general area without causing significant interference to each other.

- Many spread spectrum systems will be used indoors. The building walls will absorb much of the wireless energy before it can go very far and cause interference problems.

The first license-free spread spectrum wireless system were short-range, indoor LANs. These systems were used for applications such as retail price marking and inventory management. Next, wireless equipment manufacturers began to offer spread spectrum equipment with improved antennas systems that could be used for longer distance outdoor point-to-point links between buildings. These outdoor links offered a low-cost alternative to the expansive leased line connection offered by local telephone companies. Soon, cities, school districts and corporations began to use this outdoor equipment in point to multipoint network configurations. By the end of the century, the first Wireless Internet Service Providers (WISPs) began to provide license free broad band wireless internet access to public.

1.4 LICENSE-FREE WIRELESS FREQUENCIES

The following are the license-free spread spectrum frequencies that the wireless equipment is allowed in the ISM bands:

- 2.4 to 2.483 GHz (2.4 GHz range)
- 5.725 to 5.850 GHz (5GHz range)

1.5 ADVANTAGES OF LICENSE-FREE WIRELESS NETWORKS

- Cost savings
- Fast deployment speed
- Network architecture flexibility
- Network independence

1.6 CHALLENGES OF LICENSE-FREE WIRELESS NETWORKS

To obtain the most benefit from wireless WANs, an understanding of the challenges of their successful deployment is needed. These challenges are as follows:

- Understand wireless fundamentals
- Overcoming real-world obstacles
- Maximizing available bandwidth
- Working safely

Wireless signals are invisible to the human eye. Making this invisible phenomenon become visible requires some learning and practice.

Successful wireless deployment requires an understanding of wireless principles. These principles determine the behavior of the wireless signals, such as how they do the following:

- Spread out and get weaker as they leave an antenna and travel from point to point.
- Lose strength when they hit a tree, hill or other obstruction
- Reflect off of a building, the ground and bodies of water.

1.7 EXPLORING PRESENT APPLICATIONS FOR WIRELESS

Many corporations and industries are jumping into the wireless arena. Two of the industries most committed to deploying wireless technologies are airports and hotels, for business travelers' communications needs. If they are traveling in a car, they use their wireless phones. When they are at work or home, they are able to use their computers and resources to again be productive. But when staying in a hotel for the night or even a week, there are few choices, a business traveler can look for the RJ 11 jack and connect to the Internet via 56-kbps modem, not connect at all, or connect

wirelessly. When a hotel provides the correct configuration information based on the provider, and a software configuration, a business traveler with wireless capabilities can connect to their network without worrying about connection speed or out-of-date modems. Airports offer such services to increase travelers' productivity at a time when they would otherwise be isolated from business resources. The same configuration applies: set the configuration in the wireless client software and simple, it is connected. This wireless technology allows users to get access to the Internet, e-mail, and even the corporate intranet sites utilizing a Virtual Private Network (VPN) solution. Now, the work (or in some cases, gaming) can be done during what used to be known as idle time. This increase in productivity is very attractive to corporations who need their increasingly mobile workforce to stay connected. This scenario is accomplished using the following scheme:

- A wireless Internet service provider contracts with the airport or hotel to set up wireless access servers and access points.
- Access points are located in specific locations to provide wireless coverage throughout the hotel or airport.

Using this scenario, anyone with an account to that service provider can get access to the Internet by walking into the location where the service is offered with their laptop, Personal Digital Assistant (PDA), or other wireless device. This access includes such applications as e-mail, Intranet connection via VPN solution, and push content such as stock updates, and Web browsing. Not that this is all work and no play, it can also be set up for online gaming and video-on-demand sessions. In fact, non-work scenarios open up the possible user base to children and families, multiplying the use and demand of this technology.

1.7.1 Applying Wireless Technology to Vertical Markets

There are several vertical markets in addition to airports and hotels that are realizing the benefits of utilizing wireless networks. Many of these markets, including delivery services, public safety, finance, retail, and monitoring applications, are still at the beginning of incorporating wireless networks, but as time passes and the demand and popularity grows, they will integrate wireless networking more deeply.

a) Using Wireless in Delivery Services

Delivery and courier services, which depend on mobility and speed, employ a wireless technology called Enhanced Specialized Mobile Radio (ESMR) for voice communication between the delivery vehicle and the office. This technology consists of a dispatcher in an office plotting out the day's events for a driver. When the driver arrives at his location, he radios the dispatcher and lets them know his location. The benefit of ESMR is its ability to act like a CB radio, allowing all users on one channel to listen, while still allowing two users to personally communicate. This arrangement allows the dispatcher to coordinate schedules for both pick-ups and deliveries and track the drivers' progress. Drivers with empty loads can be routed to assist backlogged drivers. Drivers that are on the road can be radioed if a customer cancels a delivery. This type of communication benefits delivery services in two major areas, saving time and increasing efficiency. United Parcel Service (UPS) utilizes a similar wireless system for their business needs. Each driver carries a device that looks like a clipboard with a digital readout and an attached pen like instrument. The driver uses this instrument to record each delivery digitally. The driver also uses it to record digitally the signature of the person who accepts the package. This information is transmitted wirelessly back to a central location so that someone awaiting a delivery can log into the Web site and get accurate information regarding the status of a package.

b) Using Wireless for Public Safety

Public safety applications got their start with radio communications for Maritime endeavors and other potentially hazardous activities in remote areas. Through the use of satellite communications and the coordination of the International Maritime Satellite Organization (INMARSAT), these communications provided the ships with information in harsh weather or provide them a mechanism to call for help [2]. This type of application led to Global Positioning Systems (GPS), which are now standard on naval vessels. In many cases, a captain can use the 24 satellites circling the globe in conjunction with his ship's navigational system to determine his exact location and plot his course. GPS is also used for military applications, aviation, or for personal use when tracking or pinpointing the user's location could save his or her life. Today, there are medical applications that use wireless technology such as ambulance and hospital monitoring links. Remote ambulatory units remain in contact with the hospital to improve medical care in the critical early moments. An emergency medical technician can provide care under a doctor's instruction during transport prior to arriving in the hospital's emergency room. Standard monitoring of critical statistics are transmitted wirelessly to the hospital.

c) Using Wireless in the Financial World

Wireless applications can keep an investor informed real-time of the ticker in the stock market, allowing trades and updates to be made on the go. No longer is the investor tied to his desk, forced to call into his broker to buy and sell. Now, an online investor has the opportunity to get real-time stock quotes from the Internet pushed to his wireless device. He can then make the needed transactions online and make decisions instantaneously in response to the market. There are also services that allow signing up and getting critical information about earmarked stocks. In this scenario, threshold on a particular stock can be setup and alarmed. When the threshold is met, the service sends a page instantly. Again, this improves the efficiency of the investor.

d) Using Wireless in Monitoring Applications

Wireless technologies have been used for monitoring for years. There are typically two types of monitoring: passive and active. Active monitoring is conducted by use of radio signals being transmitted, and any of a number of expected signals received. An example of this implementation is the use of radar guns in traffic control. In this case, the patrolman points the gun and pulls the trigger, and a specific reading of a specific target is displayed on the radar unit. Passive monitoring is a long-term implementation whereby a device listens to a transmitter and records the data. An example of this is when an animal is tagged with a transmitter and the signal is collected and data is gathered over a period of time to be interpreted at a later date.

1.7.2 Applying Wireless Technology to Horizontal Applications

Along with the many vertical markets and applications, wireless technologies are applied to horizontal applications, meaning that delivery services, public safety, finance, retail, and monitoring can all use and benefit from them. The next section gives an overview of some of the more popular horizontal trends in wireless technology.

a) Using Wireless in Messaging

The new wave of messaging is the culmination of wireless phones and the Wireless Application Protocol (WAP) and Short Message Service (SMS). This service is similar to the America Online Instant Messaging service. The ability for two-way messaging, multiservice calling, and Web browsing in one device creates a powerful tool for consumers, while providing the vendors the ability to generate higher revenues

b) Using Wireless for Web Surfing

In addition to the standard laptop computer connected to a wireless LAN with Internet connectivity, there has been an explosion of other wireless units that offer multiple voice and data applications integrated in one piece of equipment. Typically, personal organizer functionality and other standard calculation-type services are offered, but now, these devices are used with appropriate software to get access to the Internet.

This brings the power of the Internet and the vast repository of information to the palm of the hand. PDAs, Palmtops, handheld devices, and wireless phones with the appropriate hardware and software are now being used for Internet access at speeds of up to 56 Kbps. This is moving wireless into the realm of not only browsing the Internet, which is a big accomplishment in and of itself, but Internet gaming. As the interface of the wireless devices gets better and better, the gaming community will be able to offer high quality online games played on a PDA.

1.8 BASIC ELEMENTS OF A WIRELESS NETWORK

Primarily, there are just two basic elements of a wireless network, the antenna and the wireless device. But a wireless is not a standalone network. For example, a wireless LAN is composed of access points, antennas, and wireless PC cards. The only connection that is truly "wireless" is between the antenna and the PC card. The access point is connected to the wire-line network infrastructure, and the access point is then wired to the antenna.

There are numerous types of antennas, and each type is optimized for a particular environment or application. It is important to understand the distinguishing characteristics when choosing the appropriate antenna for the wireless network design.

All radios share a basic conceptual design. In this generic design many of the specific components are commonly simplified into a "black box" schematic. Figure 1.1 highlights the generic "black box" radio components.

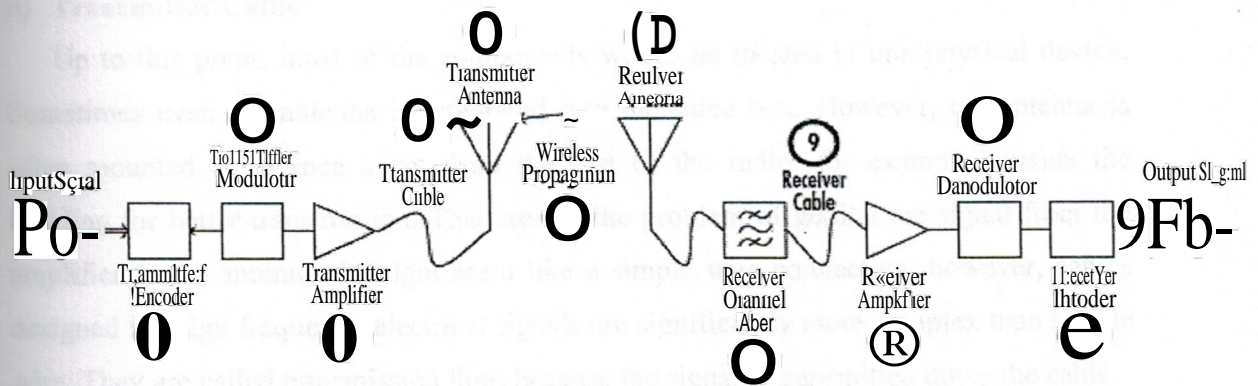


Figure 1.1 Generic Radio Components [3]

Each of the boxes in this picture represent entire subsystems of the radio; each is very complex, but simplified here as a box representing their function. The function of each of these boxes, following the system from the origin of the signal to the output of the receiver, can be described briefly as follows:

a) **Transmitter Encoder**

The input signal enters the encoder. This could be a microphone that encodes analog sound waves into analog electrical waves or it could be a complex CDMA analog-to-digital converter.

b) **Transmitter Modulator**

The modulator box performs the modulation of the carrier wave.

c) Transmitter Amplifier

After the signal is modulated, it is amplified so that it can be radiated with enough power to reach the receiving antenna.

d) Transmitter Cable

Up to this point, most of the components would be located in one physical device. Sometimes even the antenna is integrated into the same box. However, the antenna is often mounted a distance away from the rest of the radio, for example outside the building for better transmission. That creates the problem of getting the signal from the amplifier to the antenna. It might seem like a simple wire connection; however, cables designed for high frequency electrical signals are significantly more complex than simple wire. They are called transmission lines because the signal is transmitted down the cable.

e) Transmitter Antenna

The purpose of an antenna is to convert electrical signal to radio waves and vice versa. The antenna is one of the simplest subsystems of a radio because most antennas are passive devices, yet a tremendous amount of engineering goes into antenna design.

f) Wireless Propagation

The oscillating voltage potential in the antenna generates an oscillating electric field between the antenna and the ground plane. The oscillating electric field creates an oscillating magnetic field, the magnetic fields create additional electric fields, and the wave propagates away from the antenna.

g) Receiver Antenna

Similar to the transmitter antenna, the receiver antenna converts the radio waves back into an electrical signal.

h) Receiver Channel Filter

Even though antennas are designed and tuned for a specific frequency, they will still receive EM energy from the entire spectrum. Most electrical components are designed to

work at a specific range of frequencies and they do not deal well with frequencies outside this range. For this reason the received signal is filtered to allow only the intended frequencies to pass to the subsequent receiver components.

i) Receiver Cable

It is the same as the transmitter cable. On the transmitter end, the signal is amplified before leaving the main circuitry of the transmitter and entering the cable; therefore, cable loss is not a problem on the transmitter side. However, on the receiver, the weak signal can be drastically affected by loss due to the length of the cable and the quality of the cable.

j) Receiver Amplifier

The received signal is usually very weak and must be amplified before it is processed by the more complex receiver components. Some receiver designs place this amplifier or add an additional amplifier before the cable and very near the antenna to boost the received signal so that cable loss does not kill the signal as it travels from the antenna to the main receiver.

k) Receiver Demodulator

It separates the original encoded modulating signal from the carrier signal. On a clean signal, the output of the receiver demodulator should closely represent the input of the transmitter demodulator.

l) Receiver Decoder

This component decodes the demodulated signal to get a representation of the original input signal. As noise increases and/or the received signal strength decreases, the output of the receiver less resembles the transmitted signal until the point where it can no longer be recognized as the same signal.

1.9 BASIC ANTENNAS AND TYPES

By definition, an antenna is a conductive device used to transmit and/or receive radio waves. Antennas are passive devices and can be the simplest components in a wireless system. However, there is a tremendous amount of engineering and complex math that goes into designing antennas to meet certain needs.

Some antennas are designed to broadcast a signal in all directions, known as omnidirectional antennas; other antennas are designed to focus their beam in a specific direction, known as directional antennas. However, each type is optimized in certain environments. Selecting the right antenna is crucial in designing a wireless system.

1.9.1 Omnidirectional Antennas

Omnidirectional antennas propagate or receive signals in all directions. These types of antennas are useful in point-to-multipoint scenarios like a radio station, and for mobile devices that are constantly changing their aspect to their peer antenna.

a) Half-Wavelength Dipole (Half-Dipole)

The half-wavelength dipole antenna is one of the simplest antennas in design and construction. It consists of two conductors positioned end-to-end with a small gap between them. This gap usually is filled with a dielectric such as air, plastic, silicon, or rubber. The total length of the two conductors should be one half of the wavelength of the wave that they are designed to send or receive. If the antenna is designed for a range of frequencies such as the FM broadcast radio band, then the length is usually half the wavelength of the center frequency of the range. Figure 1.2 illustrates a half-wavelength dipole antenna and demonstrates its omnidirectional propagation pattern.

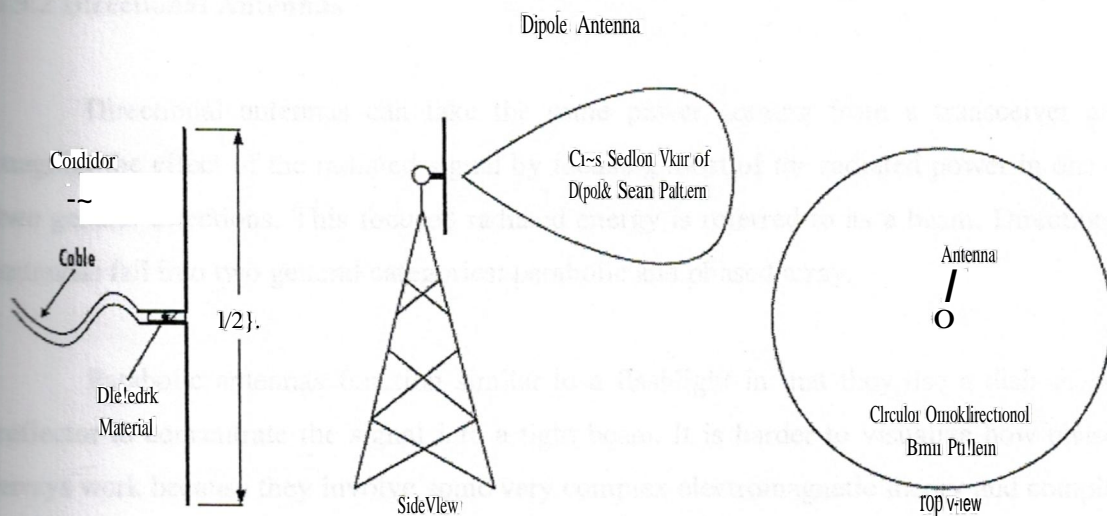


Figure 1.2 Dipole Antenna and Associated Omnidirectional beam pattern [4]

When the antenna is not near half the wavelength, the performance of the antenna is drastically affected due to a mismatch in characteristic impedances and standing wave ratios.

b) Quarter-Wavelength Dipole (Quarter 1Dipole)

The quarter-wavelength dipole is a special version of the half-wavelength dipole. It consists of one side of a half-wavelength dipole that is mounted above a ground plane, such as the roof of a car. The ground plane acts as a reflector to simulate the second arm of a half-wavelength dipole. Quarter-wavelength dipoles do not have as high of a gain as half wavelength dipoles, but they are close. Quarter-wavelength dipoles are probably the most recognized form of antennas. They are found on almost all cars and "boom boxes" for AM and FM broadcast radio reception. They are also found on most handheld transceivers such as cellular phones, wireless phones, and two-way radios.

1.9.2 Directional Antennas

Directional antennas can take the same power coming from a transceiver and magnify the effect of the radiated signal by focusing most of the radiated power in one or two general directions. This focused radiated energy is referred to as a beam. Directional antennas fall into two general categories: parabolic and phased array.

Parabolic antennas function similar to a flashlight in that they use a dish-shaped reflector to concentrate the signal into a tight beam. It is harder to visualize how phased arrays work because they involve some very complex electromagnetic theory and complex mathematics.

a) Yagi Array Antennas

Yagi antennas are named after their inventor, Dr. Hidetsugu Yagi. Yagi antennas consist of three or more dipole antennas, called elements, mounted on a common boom. All the elements work together as a phased array to direct the radiated energy into a focused beam. This gives Yagi antennas much higher gains than a half-wavelength dipole. Figure 1.3 illustrates the design and construction of a Yagi antenna. The elements are longest at the rear and gradually get shorter towards the front. The rear element is called the reflector. Immediately in front of the reflector is the driven element. In front of the driven element are one or more director elements.

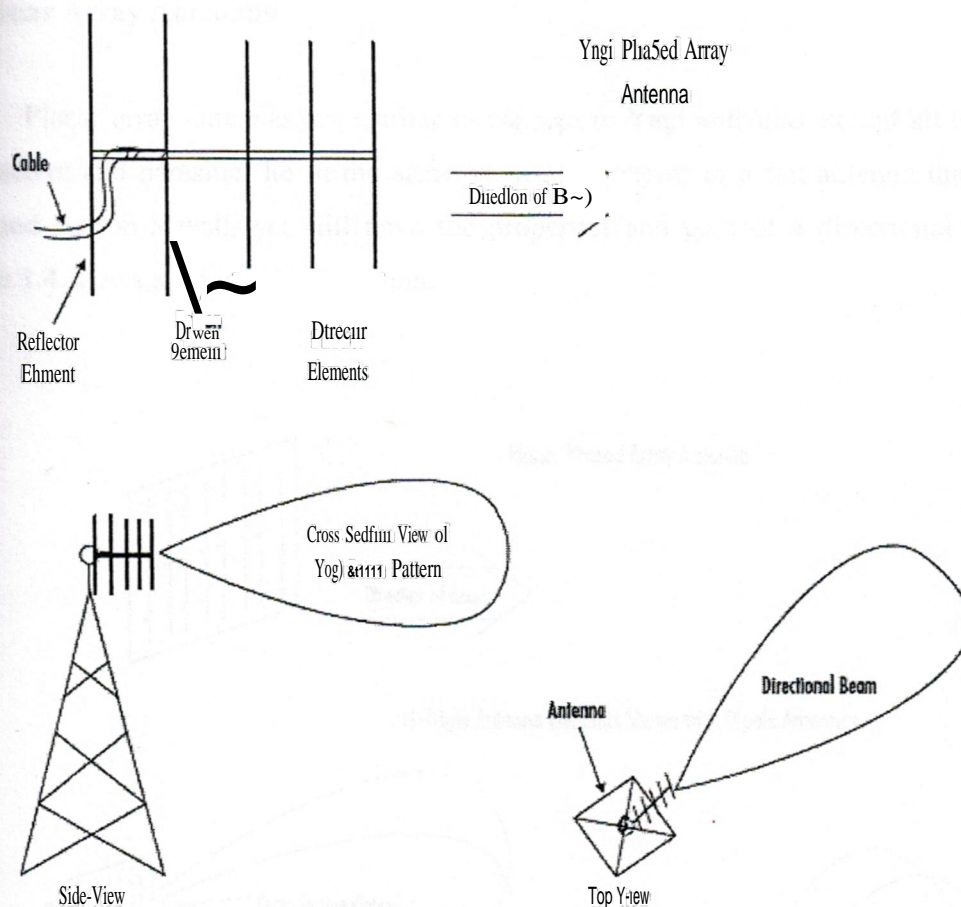


Figure 1.3 Yagi Phased Array Antenna and Associated Directional beam pattern [5]

The driven element is the only active element on a Yagi antenna and is the only element that connects to the transceiver via a cable. The remaining elements are known as parasitic elements because they feed off of the radiated power from the driven element. If a piece of metal receives a signal and it is not drained from the metal, it will be re-radiated from the metal. This is how the parasitic elements of a Yagi work. Broadcast television antennas are examples of Yagi type antennas.

b) Planar Array Antennas

Planar array antennas are similar in concept to Yagi antennas except all elements, both active and parasitic, lie in the same plane. This results in a flat antenna that can be mounted flat on a wall, yet still have the properties and gain of a directional antenna. Figure 1.4 shows a planar array antenna.

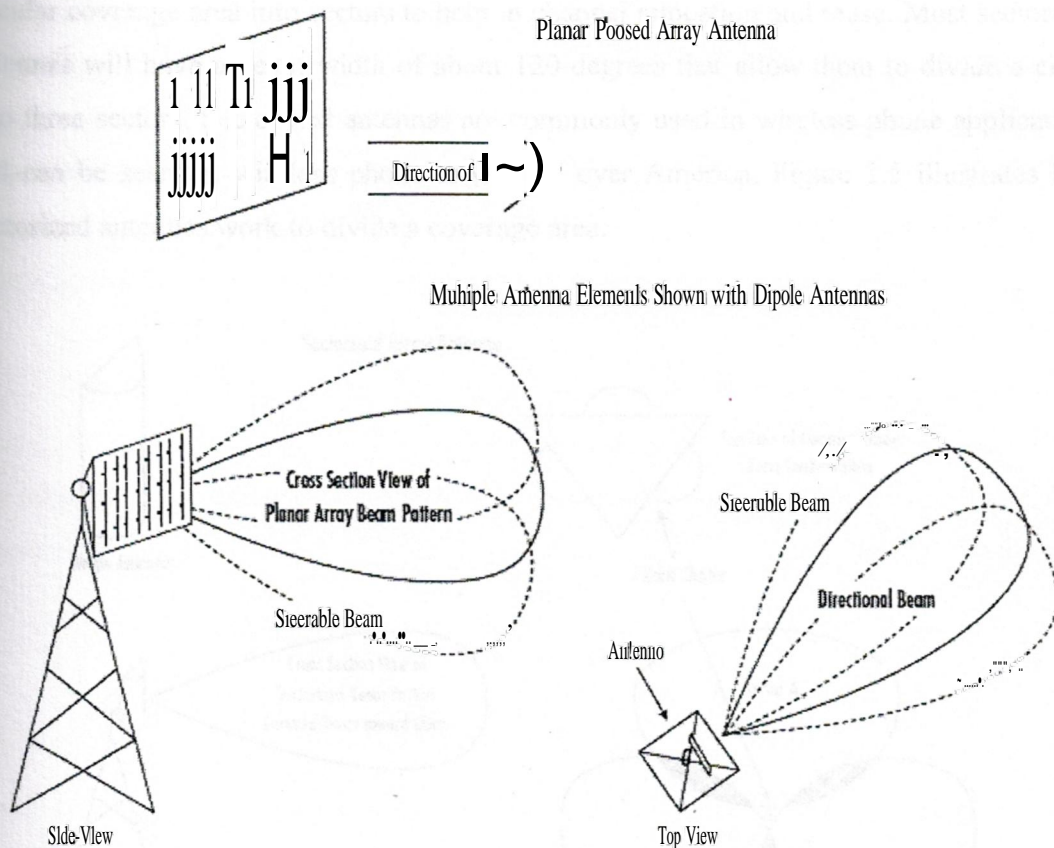


Figure 1.4 Planar Array Antennas and Associated Directional Beam Pattern [6]

Planar arrays can have more than one active element. By changing the phase and power of the signal to hit specific active elements, the beam can be steered without the

antenna physically moving. A useful application of this is on military tracking radars. A computer can adjust the input signals to the various elements of a planar array and steer the beam faster than the whole array could be moved physically, thus allowing for tracking of multiple fast-moving targets.

c) Sectorized Array Antennas

Sectorized array antennas are a type of phased array antenna designed to split up a circular coverage area into sectors to help in channel allocation and reuse. Most sectorized antennas will have a beam width of about 120 degrees that allow them to divide a circle into three sectors. Sectorized antennas are commonly used in wireless phone applications and can be seen on wireless phone towers all over America. Figure 1.5 illustrates how sectorized antennas work to divide a coverage area.

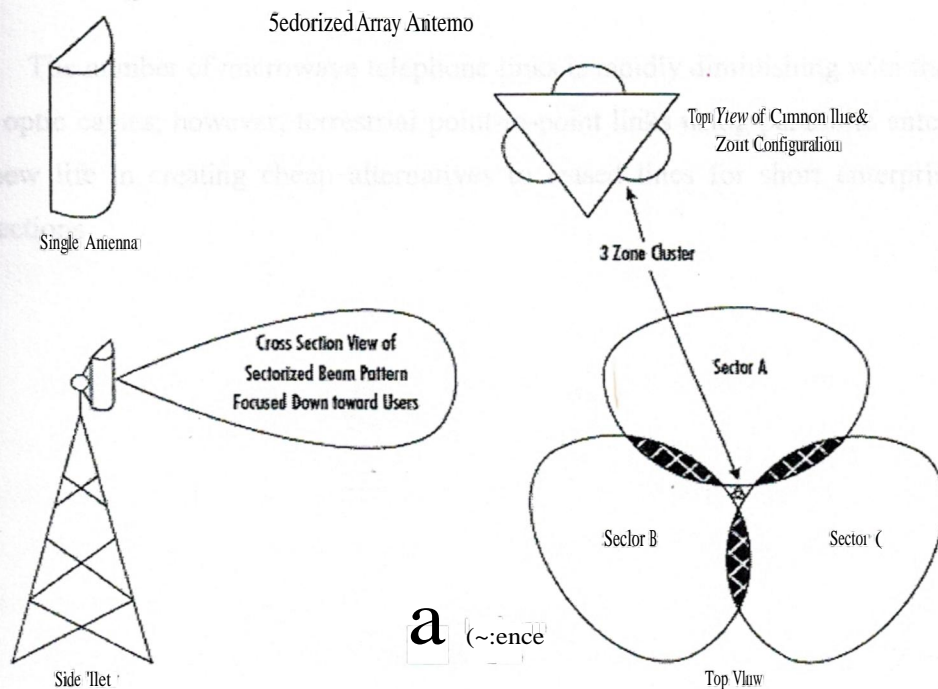


Figure 1.5 Sectorized Array Antennas and Illustration of Sectorization [7]

It is important to plan the zones carefully to minimize interference zones or to make interference zones reside in regions with no users.

d) Parabolic Antennas

The most common examples of parabolic antennas are satellite dishes. Parabolic antennas have an emitter that is mounted so that it is aimed into a bowl-shaped reflector. Just as in a car's on-off flashlight, the reflector acts to focus the signal from the emitter into a very tight beam. On the receiving end, the dish reflector increases the area of the antenna, collecting a lot more of the transmitted signal and focusing that signal back onto the receiver. Figure 1.6 illustrates how parabolic antennas work. Parabolic antennas are used for terrestrial-to-stellar communication (ground-to-satellite) and for terrestrial-to-terrestrial point-to-point communication. Microwave long-distance telephone links use parabolic and cone antennas to carry phone conversations from one point to another.

The number of microwave telephone links is rapidly diminishing with the advent of fiber optic cables; however, terrestrial point-to-point links using parabolic antennas could see new life in creating cheap alternatives to leased lines for short enterprise network connections.

Parabolic Antenna

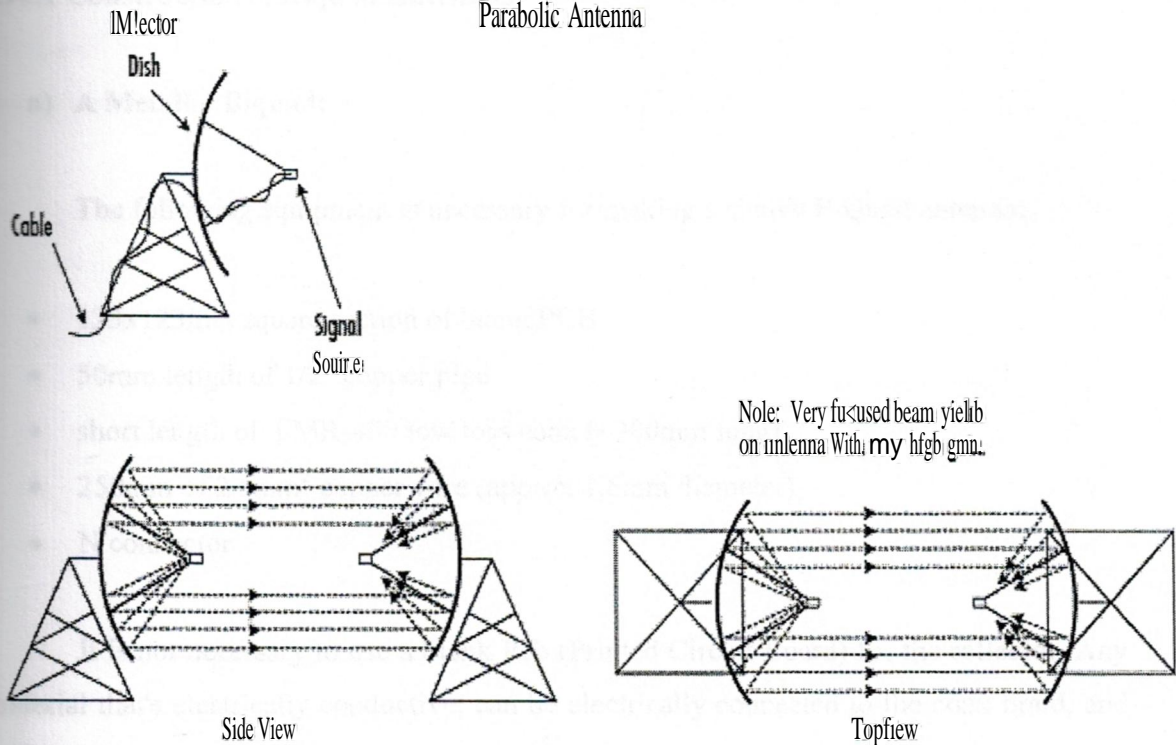


Figure 1.6 Parabolic Antennas and Focused Beam Pattern [8]

1.10 BIQUAD ANTENNA

The BiQuad antenna is simple to build and offers good directivity and gain for Point-to-Point communications. It consists of a two squares of the same size of $\lambda/4$ wavelength as a radiating element and of a metallic plate or grid as reflector. This antenna has a beamwidth of about 70 degrees and a gain in the order of 10-12 dBi. It can be used as stand-alone antenna or as feeder for a Parabolic Dish. The polarization is such that looking at the antenna from the front, if the squares are placed side by side the polarization is vertical.

1.10.1 Construction of BiQuad Antennas

a) A Metallic BiQuad:

The following equipment is necessary for making a simple BiQuad antenna:

- 123x123mm square section of blank PCB
- 50mm length of 1/2" copper pipe
- short length of LMR-400 low loss coax (~300mm long)
- 250mm of 2.5mm² copper wire (approx 1.5mm diameter)
- N connector

It is not necessary to use a blank Pcb (Printed Circuit Board) for the reflector. Any material that's electrically conductive, can be electrically connected to the coax braid, and **will** reflect microwaves i.e., any metal plate will do fine. A size of 123x123mm is recommended if using the biquad as a stand-alone antenna, while 110x110mm is optimal if using it as a feed for a large dish. Attaching some lips to two sides of the reflector reduces radiation from the rear lobes. Using some steel wool any tarnish is removed and polished. Cleaning the copper in this way will make it easier to solder (Fig 1.7)

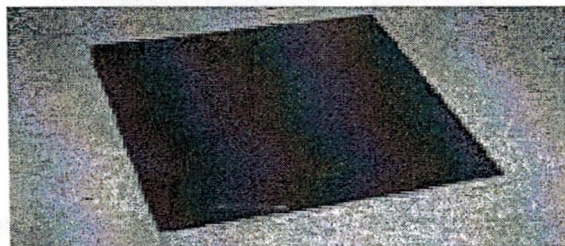


Figure 1.7 a blank printed circuit board

A 50mm section of copper pipe is cut, and both ends are smoothened. Using some sandpaper and/or some files, the copper pipe is polished up (including the inside of the copper pipe, to ensure a good connection with the coax braid).

A notch is cut into one end of the copper pipe, removing approx 2mm from half the circumference as shown in figure 1.8.

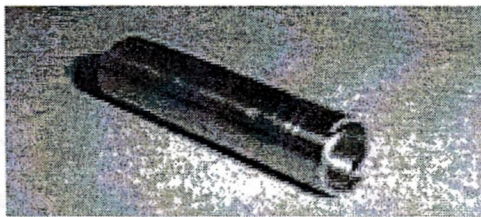


Figure 1.8 a short section of copper pipe, notched at one end

Then a hole is drilled in the centre of the blank Pcb so that the copper pipe is a tight fit in the hole as shown in figure 1.9.

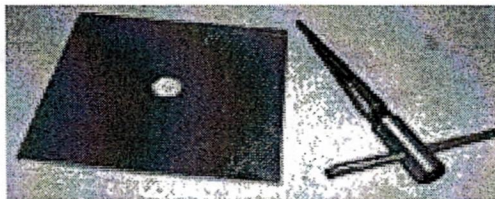


Figure 1.9 making a hole in the centre

The copper pipe is inserted into the hole, with the notched end on the copper side of the blank Pcb. The copper pipe should be protruding approx. 16mm through the hole (Fig 1.10) measured on the copper side of the Pcb.

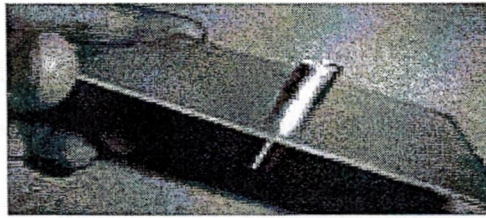


Figure 1.10 inserting the copper pipe into the reflector

Then, the copper pipe is soldered to the Pcb, to ensure a good physical and electrical connection. The element is made from a length of copper wire, bent into the appropriate shape. The length of each "side" should be as close to 30.5mm as possible (measured from the centre of the copper wire to the centre of the copper wire), which is a quarter of a wavelength at 2.4GHz (Fig 1.11).

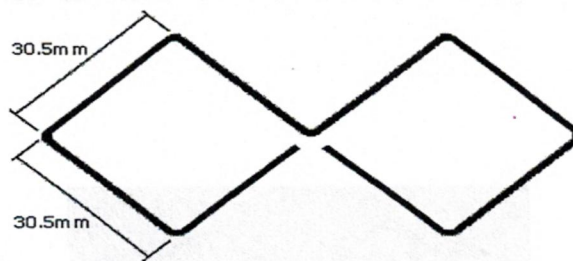


Figure 1.11 the shape and dimensions of the element

After that, a copper wire is taken, from any electrical power cable and the insulation was removed, measured and 244mm length the copper wire was cut and straightened as best as it could (Figure 1.12).



Figure 1.12 straightening the wire

The mid-point of the wire is measured, and a 90 degree bend is made. The bend should be quite sharp and pronounced. Then the midpoints of each half are measured, and two more 90 degree bends are made in the wire, so that it looks like that shown in the figure 1.13.

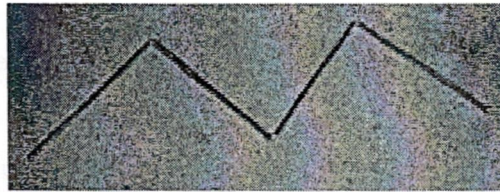


Figure 1.13 another two bends

Once again, the midpoints of each section are measured, and made some more 90 degree bends, and doing the same to the other side, resulting in the biquad shape as in figure 1.14.

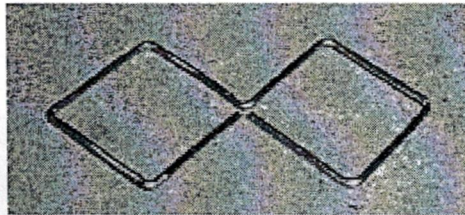


Figure 1.14 A symmetrical BiQuad element

The element must now be attached to the reflector. It is important that only the two "ends" of the copper wire are to be attached to the copper pipe - the centre of the copper wire must not touch the copper pipe. The copper wire should be approximately 15mm away from the reflector as shown in figure 1.15.

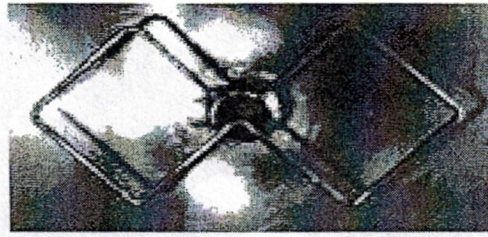


Figure 1.15 the element soldered onto the copper pipe

Now, approx 30mm of the outer sheath is stripped from the end of the coax (Figure 1.16), the braid back was folded over the outer sheath and the centre conductor is trimmed so that about 4mm is protruding (Figure 1.17)

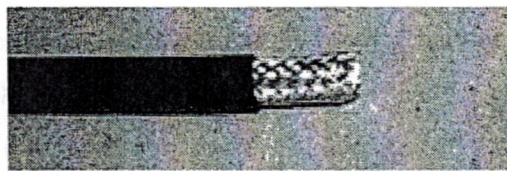


Figure 1.16 the outer sheath is stripped

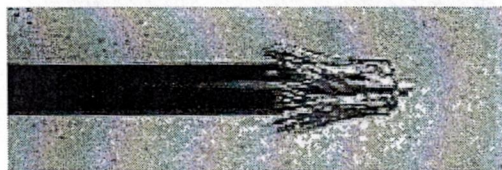


Figure 1.17 the braid is folded back, trimming the centre conductor

The braid is inserted into the copper pipe, so that the ends of the centre conductor lines up with the extreme end of the copper pipe, and solder the centre of the element to it, ensuring the centre of the element is not in contact with the copper pipe as in figure 1.18.

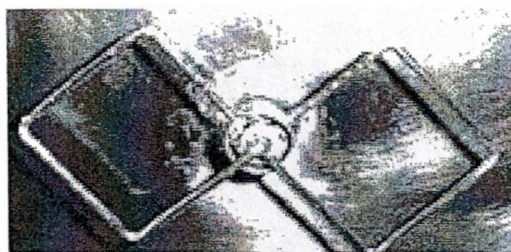


Figure 1.18 soldering the centre conductor to the element

After this, the other end of the coax is fixed with an N connector. If it is intended to mount the biquad outside, it is recommended that the antenna is placed into a weather-proof enclosure, to prevent corrosion, and to prevent water ingress into the coax.

This can be achieved by drilling a hole in one side of the container, and passing the coax tail through the hole, leaving the biquad itself inside the container as in figure 1.19. Sealing up the hole for the coax with some silicone, and the biquad should be protected against the elements.



Figure 1.19 a view of the completed biquad

Similarly a Biquad with 50 degree directivity can be achieved by adding clips to the side of the reflector, 20mm high on both ends as shown in the figure 1.20.

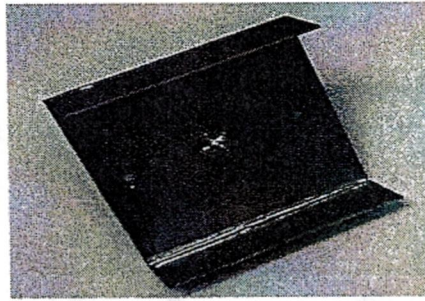


Figure 1.20 A Vertical Biquad with added directivity

When using a biquad to establish a link to another wireless device, it should be ensured that the polarization of the biquad is the same as the antenna connecting to. Similarly, if establishing a link with two biquads, it should be ensured they are both oriented for the same polarization as in figure 1.21. Failing to match the polarizations will result in significant signal loss.

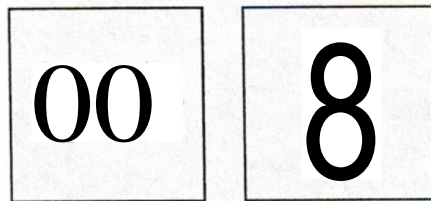


Fig 1.21 A vertical polarity and a horizontal polarity of the BiQuad

Changing the polarizations is just a matter of rotating the entire biquad antenna by 90 degrees. The biquad antenna is not particularly directional, but has a fairly wide beamwidth.

b) A Pcb Biquad:

A successful Biquad can be manufactured using a Pcb as shown in figures 1.22 and 1.23.

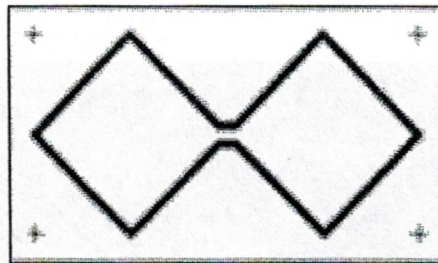


Figure 1.22 The copper lamination on a PCB board



Figure 1.23 a Pcb Biquad Antenna

The exact specs of the element are laminated on top of the circuit board at exact 30mm each, thus minimizing errors as low as possible. The braid of the cable is soldered to one end of this copper lamination on the Pcb and the other end of the coaxial cable to the other end, thus making a complete Pcb Biquad.

c) A Dual Biquad

The copper wire is bent at exactly 30.5mm apart, thus giving it a helix shape with two biquads attached together as shown in the figure 1.24.

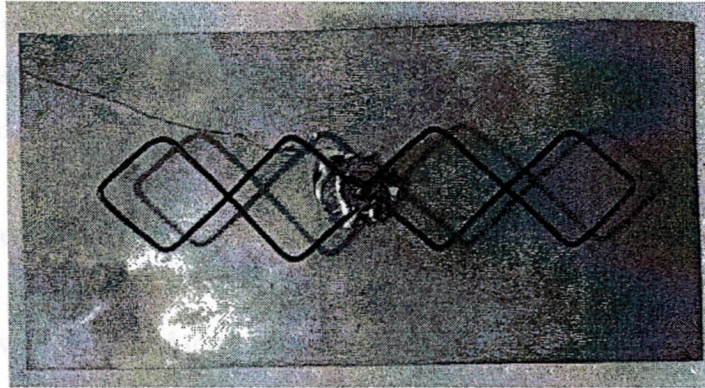


Figure 1.24 A Dual Biquad

The same procedure is repeated with the cable soldering as in the metallic Biquad, and thus, a dual Biquad is manufactured. The back reflector is spaced at about 15mm to have the highest gain in this antenna. The dimensions of the back reflector are 200mm x 170mm.

1.10.2 Comparisons and Testing

For the purpose of comparison and testing, the following equipment was used

- 1- A Patch Antenna (13.2 dBi)
- 2- Transmission cable
 - a) LMR 195 cable (Loss in cable is 0.6 db/m)
 - b) LMR 400 cable (Loss in cable is 0.22db/m)
- 3- Four Prototypes of Biquad Antenna

- a) A metallic Biquad
- b) A Biquad with 20mm clipping
- c) A Pcb Biquad
- d) A Dual Biquad
- 4- D-link Access Point (2pcs)
- 5- Simulating and monitoring software
 - a) Enterasys Client Utility
 - b) Minitar WLAN Client utility
 - c) D-Link Airplus Utility
- 6- Two Laptops with XP operating system and Ethernet ports
- 7- Ethernet cables with RJ-45 jacks

The biquads were tired and tested against a 13.2dBi Patch Antenna as shown in the figure 1.25.

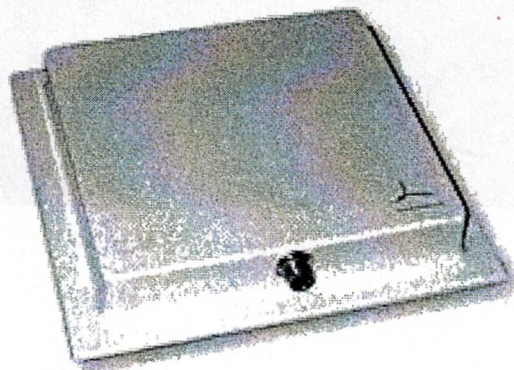


Figure 1.25 A 13.2 dBi Patch Antenna

For comparison purposes, an 11 MHz link was established with a laptop at both ends which was almost a kilometer apart. At one end, an omnidirectional antenna was installed which had the 360 degree radiation pattern, and on the other end, the prototypes were used one by one and the calculations were noted accordingly. The D-link Access point was used at both ends to acquire the beam pattern and signal strength. A PCMCIA

card could also be used but, most of the PCMCIA cards do not come with the connectors for LMR 400 and LMR 195 cables, so a D-Link Access Point served the purpose and was connected to the laptop by using an RJ-45 Jack Ethernet cable.

a) Testing for Signal Strength

First, Enterasys Client Utility was used to monitor the signal to noise ration (SNR) of the Patch antenna and the prototypes. For each test, the prototypes were monitored for almost 90 seconds. A screenshot of Enterasys Link Test is shown in the figure 1.26.

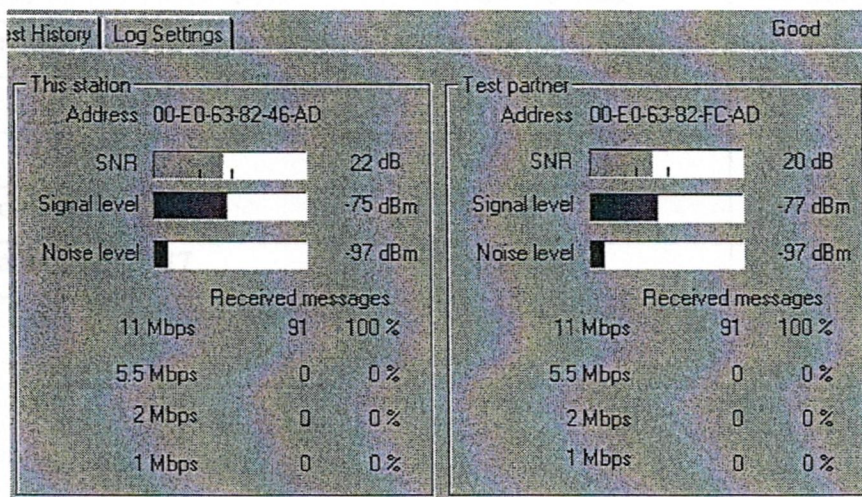


Figure 1.26 Enterasys Link Test

1- Using LMR 195 cable (For Horizontal Polarity)

The antennas were tested for the horizontal polarity and the results were depicted in the table 1.2.

	Signal (dBm)	Noise (dBm)
Patch Antenna	-75	-101
Biquad 1	-80	-105
Biquad 2	-80	-102
Peb Biquad	-80	-102
Dual Biquad	-80	-100

Table 1.2 Enterasys Link Test results for Horizontal polarity using LMR 195

Laptop A			
Antenna Type	SNR(dB)	Signal (dBm)	Noise (dBm)
Patch Antenna	49	-55	-98
Biquad 1	42	-58	-100
Biquad2	44	-57	-99
Pcb Biquad	42	-59	-101
Dual Biquad	48	-55	-99
Laptop B			
Antenna Type	SNR(dB)	Signal (dBm)	Noise (dBm)
Patch Antenna	47	-57	-97
Biquad 1	41	-59	-101
Biquad 2	42	-58	-100
Pcb Biquad	42	-58	-101
Dual Biquad	47	-57	-99

2- Using LMR 195 (For Vertical Polarity)

Then the antennas were tested for the vertical polarity as shown in the table 1.3.

Table 1.3 Enterasys Link Test results for vertical polarity using LMR 195

Laptop A			
Antenna Type	SNR(dB)	Signal (dBm)	Noise (dBm)
Patch Antenna	46	-55	-101
Biquad 1	40	-60	-103
Biquad 2	41	-60	-102
Pcb Biquad	40	-60	-102
Dual Biquad	45	-56	-100

Laptop B			
Antenna Type	SNR (dB)	Signal (dBm)	Noise (dBm)
Patch Antenna	45	-55	-100
Biquad 1	40	-61	-102
Biquad 2	40	-60	-101
Pcb Biquad	41	-59	-102
Dual Biquad	45	-55	-103

3- Using LMR 400 cable (For Horizontal Polarity)

The antennas were again tested and tried for the Horizontal polarity using the LMR 400 cabling, as shown in table 1.4.

Table 1.4 Enterasys Link Test results for Horizontal polarity using LMR 400 cable

Laptop A			
Antenna Type	SNR(dB)	Signal (dBm)	Noise (dBm)
Patch Antenna	51	-52	-97
Biquad 1	43	-57	-99
Biquad 2	45	-56	-99
Pcb Biquad	43	-56	-98
Dual Biquad	50	-50	-97
Laptop B			
Antenna Type	SNR(dB)	Signal (dBm)	Noise (dBm)
Patch Antenna	50	-53	-96
Biquad 1	44	-57	-99
Biquad 2	45	-57	-101
Pcb Biquad	45	-57	-102
Dual Biquad	49	-54	-103

4- Using UvIR 400 cable (For Vertical Polarity)

And similarly the antennas were again tested for the vertical polarity using the LMR 400 cable as shown in table 1.5.

Table 1.5 Enterasys Link Test results for Vertical polarity using LMR 400 cable

Laptop A			
Antenna Type	SNR(dB)	Signal (dBm)	Noise (dBm)
Patch Antenna	49	-54	-101
Biquad 1	45	-57	-103
Biquad 2	45	-57	-102
Pcb Biquad	45	-57	-102
Dual Biquad	49	-54	-100
Laptop B			
Antenna Type	SNR(dB)	Signal (dBm)	Noise (dBm)
Patch Antenna	50	-54	-100
Biquad 1	44	-58	-102
Biquad 2	45	-58	-101
Pcb Biquad	44	-58	-102
Dual Biquad	49	-54	-103

b) Throughput Test

For monitoring the throughput test, the antennas are allowed to transmit and receive a bulk of data, and the tools are applied at the same instant with the ping test to check the feasibility of the connection and the throughput at a given time instant.

1- Using Minitar WLAN Client Utility

The throughput test can be done using a monitoring software and checking the feasibility of the transmission using the ping test at the same time. Table 1.6 show the readings taken by the experimentation.

Table 1.6 The Throughput test using Minitar WLAN client utility

Antenna	Link Quality	Signal Strength	Ping Test	Timeouts
Patch Antenna	94	79	<Ims>- lms	Oms
Biquad 1	81	69	<Ims+-Bms	Oms
Biquad 2	82	71	<Ims-4ms	Oms
Pcb Biquad	81	68	<Ims+-Yms	Oms
Dual biquad	92	77	<Ims+-Ims	Oms

2- Using D-Link Airsupply utility

Similarly, using a D-Link Airsupply utility, the throughput test was again performed and the readings were noted in the table 1.7.

Table 1.7 The Throughput test using D-Link Airsupply utility.

Antenna	Link Quality	Signal Strength	Ping Test	Timeouts
Patch Antenna	95	81	<Ims > lms	Oms
Biquad 1	80	68	<Ims-9ms	Oms
Biquad 2	83	70	<Ims=-Zrns	Oms
Pcb Biquad	81	68	<Ims-9ms	Oms
Dual biquad	94	78	<Ims=-Ims	Oms

1.10.3 Conclusions

From, Enterasys Client Utility tests (Tables 1.2, 1.3 1.4 1.5), it can be easily seen that the Antennas have a higher SNR, when they are horizontally polarized. The one obvious reason which is due to the presence of other vertically polarized omnidirectional antenna some where close. It was then confirmed by the site survey that there were more than 6 vertically polarized antennas that might have affected the quality of the signal in this testing because the signal levels at the same polarization make interference with each other and hence decrease the efficiency of transmission.

Secondly, it can also be concluded that the antennas show more signal strength when they are tested with a LMR 400 cable instead of a LMR 195 cable. It is already known that the LMR 195 has a loss of 0.6 dB/m as compared to LMR 400 which has a loss of 0.22 dB/m. Hence, it is proved that the LMR 400 is a better option when comes to antenna cabling.

Making the patch antenna as the point of reference, the isotropic power of the antennas was calculated which were:

- 1- Patch Antenna = 13.0 dBi
- 2- Biquad I = 9.0-9.5 dBi
- 3- Biquad 2 = 9.5 dBi
- 4- Pcb Biquad = 9.0 - 9.5 dBi
- 5- Dual Biquad = 12.5 - 13.0 dBi

The theoretical power levels of a stand alone Biquad antenna is 9.5 dBi to 11 dBi. In the tests, biquad # 2 came closer to the theoretical power levels as compared to the other prototypes. Further more, it is clear that the dual biquad came closer to the patch antenna in terms of performance and feasibility, as compared to other stand alone biquads.

From the throughput test, it was noticed that the ping times increased from 1ms to as high as 9ms when the data transfer was at its peak, but the patch antenna and the dual biquad showed a very strong through put, hence making them ideal for deploying in a large customer location, such as hotels and Internet Cafes.

The reason that a hand made dual biquad fares nearly as good as an industrially manufactured patch antenna, is because of the fact that, the patch comes with a female connector attached to its bottom, which requires a male N-Type connector to go with it. It decreases the gain of the signal by 0.5 db/m per connector used in the cable. The antenna prototypes used did not had this additional connector as it might have noticed, thus making the antennas stable and easily deployable.

1.11 SUMMARY

In this chapter, the differences between a traditional wired and a wireless network, along with its earlier phases of development and advantages in horizontal and vertical markets were studied. Furthermore, the necessary elements which constitute a wireless network and some basic types of antennas were also outlined. Then some prototypes of Biquad antennas were manufactured and successfully tested and compared to an industrial antenna and the results were outlined.

2. THE INTERNET PROTOCOL IN A WIRELESS NETWORK

2.1 OVERVIEW

In this chapter, a deep insight is taken into the Internet Protocol (IP), how the computers commute in a wireless network using this protocol is explained along with its properties and responsibilities.

2.2 INTRODUCTION TO INTERNET PROTOCOL

The Internet Protocol (IP) is one of the most important protocols for communication among computer systems. IP is a network layer protocol. Because each layer provides services for the layer above it, IP facilitates the communication of information from the transport layer protocols, such as TCP and UDP.

With all the responsibility this protocol carries, it functions as a best effort delivery system. Like UDP, it is a connectionless protocol, and with that comes unreliability. (The term connectionless refers to the fact that there are no record-keeping responsibilities within this layer.) However, this does not imply that the system is ineffective-rather, it relies on the upper layers to provide reliability. TCP is most commonly the transport protocol of choice for data that requires guaranteed delivery to its destination. The packets might not all reach the destination in order, but TCP ensures that they are all received. The transmission of data takes place in milliseconds, so if the receiving device has to reorganize the packets into sequential order, that is usually not perceived by the end user. The contents of the IP header are illustrated in Figure 2.1.

V4	Header Length	Type Of Service	Packet Length
Identification			
Time To Live		Protocol	Checksum
Source Address			
Destination Address			
Options			
Data			

Figure 2.1 IP Header

The IP header includes the following fields:

- V4 - The version of the Internet Protocol being used (IPv4).
- Header length (in bytes) - The number in bytes that the header occupies.
- Type of service (TOS) - Consists of four bits representing minimization of delay, maximization of throughput, maximization of reliability, and minimization of cost. Only one of these priorities can be active. The most beneficial priority depends on the application: A Simple Network Management Protocol (SNMP) packet containing information about a link failure would benefit from a maximization of reliability.

- **Packet length** - This field is included because some network access protocols pad, or add stuff bits to, a small packet in order to meet the minimum size requirement.
- **Identification** - Assigned to each packet to provide a unique identity. This field is important with fragmentation, because the identifier is duplicated in each fragment of the packet. Flags are also used to identify fragments. Fragment offset identifies the sequence of a particular fragment in relation to the beginning of the original packet.
- **Time to live (TTL)** - The number of hops a packet can travel before being discarded. This is a way of preventing routing loops.
- **Protocol** - This field identifies the protocol that generated the data in the packet.
- **Checksum** - A metric used by the receiving device to ensure that the information in the header is not corrupted on receipt.
- **Source address** - The sender's IP address.
- **Destination address** - Indicates the address of the intended recipient.
- **Options** - This field can be used to provide information about the routers, such as addresses and timestamps that the packet encounters in its path to the destination.

2.3 IP ADDRESSING

IP addresses identify both a specific network and a specific device. The network identifier is the same for all devices on the same network. However, the device identifier is unique. The entire IP address consists of 32 bits, which appear as one large binary number to computer devices. However, in order to simplify this massive number, it is broken into

four octets. Each octet is eight bits long. To further simplify IP addresses, they are represented in decimal format. In decimal, each octet ranges from 0 to 255. It is important to understand how to count in binary to design an IP architecture. This is a totally different way of counting and requires practice. Table 2.1 shows how to count in binary.

Table 2.1 Counting in Binary

Binary	Equivalent
00000000	0
00000001	1
00000010	2
00000011	3
00000100	4
00000101	5
00000110	6
00000111	7
00001000	8
00001001	9
00001010	10
00001011	11
00001100	12
00001101	13
00001110	14
00001111	15
00010000	16
00100000	32
01000000	64
10000000	128

The counting can be continued until a binary number of all 1s or eight consecutive 1s: 11111111 is reached. This number is equivalent to 255, which is the largest number any octet can be. If an increase is required from 256, it would require an additional digit (for a total of nine digits), which is larger than allowed.

As stated earlier, an IP address is a 32-bit number, broken down into octets. The way an IP address is written is in the form XXXX, where X is a number between 0 and 255.

Remembering that an IP address identifies both a network and a host; the network portion of the address is divided into three classes, to accommodate the number of hosts on a particular network:

Class A - Designed for large networks. The network portion is contained within the first octet. Consequently, the host portion of the address consists of the remaining three octets. In other words, there is a possibility for 128 autonomous or unique networks, each having the potential of 16,777,216 devices.

Class B - Designed for medium-sized networks. The network portion is contained within the first two octets. As a result, there are two remaining octets for the devices attached to the network. So, there is a potential of 16,384 different networks, each with 65,536 devices.

Class C - Designed for small networks. The network portion is three octets, and the host identifier is within the last octet. This is the most abundant group of networks, totaling 2,097,152. Networks of this class comprise no more than 256 devices.

Table 2.2 Quick and Easy Rule of the First Octet

Class	First Octet Rule	Decimal	Binary
A	First bit 0	0-127	00000000-01111111
B	First Two bits 10	128-191	10000000-10111111
C	First three bits 110	192-223	11000000-11011111
D	First four bits 1110	224-239	11100000-11101111
E	First four bits 1111	240-255	11110000-11111111

Furthermore, within each class is an address range reserved for private addresses. The private addresses are as follows: 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, and 192.168.0.0-192.168.255.255. In many cases, these addresses are designated for devices that will not be sending or receiving traffic outside their own networks. Another possible application for private addresses is a situation in which only a limited number of people would be communicating outside their network at any one time. In this case, an address pool would be established in which addresses are dynamically assigned to a device for a limited time. This is a measure to help conserve address space. These few private address ranges, along with a few others, are the only addresses that are not permitted on the Internet.

2.4 CONSERVING ADDRESS SPACE WITH VLSM

It was identified early in the development of the Internet that the limited number of IP addresses would eventually run out, so a method of splitting classes into smaller blocks needed to be developed. Conservation efforts are absolutely necessary. A large telecommunications company, which might support voice and data, means that it might have a Frame Relay network, an ATM network, an IP network and so on. Not only specific addresses for the equipment are needed, but it must also supply its customers Internet services along with address space for their equipment. It quickly becomes apparent how

address space is rapidly being depleted. One measure to conserve address space is called *Variable Length Subnet Mask (VLSM)* [9]. The default address mask is represented in Table 2.3. (Class A address uses the first octet for the network portion, Class B the first two octets, and Class C the first three octets.)

Table 2.3 Default Address Masks

Class	Address	Default Mask
Class A	11111111.00000000.00000000.00000000	255.0.0.0
Class B	11111111.11111111.00000000.00000000	255.255.0.0
Class C	11111111.11111111.11111111.00000000	255.255.255.0

It can be said that an address of 192.168.1.1 is a Class C address, since it falls between the range of 192 and 223. Given in table 2.3, it is seen that the mask for this address is 255.255.255.0. This is also noted as a /24, which represents the number of 1 bits in the mask. It is also seen that there are three entire octets containing one bit ($8 \times 3 = 24$).

VLSM allows us to make the address mask a value other than the default ones. If relied on the default address masks for the Internet addressing, only 2,113,664 networks would be allowed on the Internet. Two million networks might sound like a lot, but with standard address masks, most would be networks with only 254 devices. With VLSM the number of networks can be extended on the Internet and allow for several different network sizes.

If an address of 192.168.0.0/26 is observed, to calculate the mask be in binary format, there will be 26 one bits:

11111111.11111111.11111111.11000000 = mask

11000000.10101000.00000000.00000000 = address

Now, how it is known that which part of the address is the network portion and which is reserved for hosts? A line is drawn after the last 1 bit in the mask and carries it through the address. This line will show how many hosts are available for the network. It's known that the first two bits in the last octet are 1s, so they are part of the network. The maximum for one octet is 255 and the first two bits are equal to 192. Therefore, $255 - 192 = 63$, and that gives us the maximum number of hosts on this /26 network.

The broadcast address for the network can also be calculated. It is known that the network portion is 192.168.0.x and, the available hosts are 192.168.0.0-192.168.0.63. In order to tell what the broadcast address is for this particular network, following procedure is done:

11111111.11111111.11111111.11 000000 = mask

11000000.10101000.00000000.00 000000 = network address

00000000.00000000.00000000.00 111111 = broadcast address

As illustrated, the network broadcast address is at the top of the range for network hosts. In this example, the broadcast address is 192.168.0.63. Furthermore, it is general practice to assign the default gateway to the first available host address. Continuing with the same example, the default gateway would be 192.168.0.1. The ability to identify the network and host range of an address is useful in troubleshooting.

2.5 IP ROUTING

Routing is responsible for moving information along an optimal path through a network. The router determines the best path using routing algorithms, which calculate the path based on certain metrics. The types of metrics used in calculating the path depend on the algorithm, and each protocol uses a different algorithm. This allows the network designer some choices in designing a network to fit the needs of the users. For instance, in banking, money transactions need to be error-free upon delivery, so speed is of a lesser

priority than reliability. Another situation with totally different needs is video streaming. Speed is the number-one priority here. Reliability is, of course, desirable, but error-free doesn't mean a lot when delay dominates the show.

5) Distance Vector and Link State Routing

a) Static and Dynamic Routing

The first decision in choosing a routing protocol is based on the complexity of the network. A small, simplistic network might be best suited for a statically routed network. Static routing is configured by a network administrator; its rules do not change unless the administrator chooses to change them. No algorithm is associated with static routing because path determination is the responsibility of the administrator. The strength of static routing is in its reliability. For example, the amount of traffic on a link can be somewhat controlled by the administrator. This is possible because if there are relatively few users, traffic flow is more predictable. In a situation in which the demands of users, and subsequently the traffic flow, are continually changing, dynamic routing is the best solution.

A dynamically routed network utilizes algorithmic calculations to adjust to network changes. A possible network change could occur when a financial officer is putting together a quarterly report. Perhaps he or she is downloading large files from various sources. This process might consume a considerable amount of bandwidth. Consequently, the traffic from other network users might need to be routed to a different link. A dynamically routed network is capable of facilitating these types of changes.

There are also routing tables, which contain the information from routing update messages. The update messages are sent either periodically or when a network change occurs, depending on the protocol. The algorithm uses the information in the routing table for path determination. In conjunction with the routing table, the algorithm uses metrics such as path length, throughput, speed of the link, and amount of traffic on a link.

Static routing is fine for a small, simple network. However, it becomes increasingly difficult to manage as the network grows, especially when problems arise.

b) Distance Vector and Link State Routing

There are basically two groups of routing protocols, distance vector and link state. The distinguishing properties are how the two groups learn about a network (specifically, the routes within a network), the algorithms that are used, and the associated metrics.

Distance vector routing learns by the rumor method. In other words, an adjacent router sends its routing table to its neighbor. The neighbor accepts the received table as trustworthy and merely adds its information to the table. In essence, routers-running this type of protocol learn only about the relative distances, in terms of hop count, of their neighbors to the nodes in a network. (Hop count refers to the number of routers a packet must encounter on the way to its destination.) The router does not know anything about the other routers in the network beyond its adjacent neighbors. The primary concern of the router is to route a packet to the next hop. It looks up the destination address in its routing table and decides which neighbor is closer to the destination.

2.6 THE INTERNET CONTROL MESSAGE PROTOCOL

Internet Control Message Protocol (ICMP) is designed to provide diagnostic and troubleshooting information and tools in order to manage an IP network. A variety of messages are provided by this protocol, indicating errors as well as query and response. Examples of common triggers for ICMP messages are when a destination is unreachable or when a request has timed out. Two tools in particular that are useful for troubleshooting are ping and traceroute.

Ping is used to check the end-to-end connectivity of a host to a remote device. An echo message is sent to the remote device. If there is connectivity, the device sends back

echo reply messages. If at least one echo reply is sent, the remote device is considered still "alive". The health of the connection is also indicated by the ratio of echo messages to echo replies. If the ratio is not one to one, the echo messages are timing out due to excessive delay in the connection or packet loss. This process is equivalent to sonar for computer systems.

Traceroute provides a packet-tracking system. This tool allows the user to see every hop, or IP address, along the path to the packet's destination address. If there are connectivity problems, this tool will show where the packet is being dropped. This tool also shows the time lapse between hops, which is helpful in detecting network congestion and the resulting delay.

2.7 UNDERSTANDING THE HOST-TO-HOST LAYER

The host-to-host layer is identical to the transport layer in terms of functionality and the protocols that reside in this layer. In order to avoid redundancy, two of the most commonly implemented protocols, UDP and TCP will be discussed in detail.

a) User Datagram Protocol

UDP is preferred for dealing with time-sensitive applications. For example, on having a conversation with someone when all of a sudden he or she tells us some fragment of information just remembered from a previous topic-and then he or she continues with the current topic. The information from the past topic has now confused the current topic. This event does not occur in UDP, because the sender assumes that all the packets are received and will not retransmit information. In addition to having time sensitivity, an advantage of UDP is reduced overhead in both the packet header and the absence of acknowledgments. As illustrated in Figure 4.2, the UDP header is quite simple

Source Port	Destination Port
Length	Checksum

Figure 2.2 UDP Header

The IP header includes the following fields:

- Source port number Indicates the sending application.
- Destination port number Indicates the receiving application.
- Length The size of the header and attached data, if any.
- Checksum (optional) includes a metric for both the header and any data.

a) Transmission Control Protocol

TCP uses three primary mechanisms to achieve reliable transmission of information: packet numbering, acknowledgments, and windowing. The importance of these attributes is evident when you look at the header, shown in Figure 4.3, where each has a dedicated field.

Source Port		Destination Port	
Sequence Number			
Acknowledgment Number			
Header Length	Reserved	Flags	Window
Checksum			Urgent Pointer
Options			
Data			

Figure 2.3 TCP Header

Packet numbering ensures sequential delivery of packets to the destination. Acknowledgments provide a method of record keeping. When a packet is received, the receiver sends an acknowledgment back to the sender. If the packets are received out of sequence, implying a loss of packet(s), or if errors are detected, an acknowledgment is not sent. In this case, the sender will retransmit the packet(s). Windowing is a measure of flow control. In other words, the sender and receiver agree on the number of packets the sender will transmit before waiting for an acknowledgment. This system provides reliability without compromising the amount of throughput by acknowledging every single packet.

There is constant communication between the sender and the audience, thus creating a virtual point-to-point connection. This method of transport is advantageous in a data environment, where each piece of data is vital.

Since this protocol is connection-oriented, a connection must be established among the devices that want to exchange data. The establishment of this connection is often referred to as a handshake process. Once the device has established a TCP session with the remote device, the devices establish certain parameters such as windowing size, and information is exchanged. Once the session is complete, the two devices must terminate the session.

As mentioned earlier, the overhead in the header alone is greater for TCP than UDP:

- **Source port number** Identifies the sending application.
- **Destination port number** Identifies the receiving application.
- **Sequence number** Identifies where a particular packet fits in the data stream. This field provides information similar to the fragment offset field in an IP header.
- **Acknowledgment number** Provides the receiving device with the sequence number of the following packet the device should be expecting.
- **Header length** This field indicates the size of the header in bits. Since there might or might not be information in the options field, it provides the media access protocol a value to compare with the minimum required size and determine if there is a need for filler bits.
- **Flags bits** Provides additional information about the header or the session itself.
- **Window size** Indicates the number of bytes the receiving device should expect before sending an acknowledgement message. This is a key field for flow control.

- **Checksum** Provides information to the receiver to verify the validity of the information in the TCP portion of a packet.
- **Urgent pointer** This is valid only if the flag field turns it on. When it is activated, it provides a way of interrupting the original data stream to send urgent information. The pointer tells the receiver where in the data stream the urgent information resides.
- **Options** An example of this field is time stamping.

2.8 MANAGING THE APPLICATION LAYER

The Department of Defense summarized the top three layers of the OSI model into a single application layer. If the operation and function of the session are taken into consideration, presentation, and application layers together, it can be concluded that they perform different pieces of the same function: providing the link between the host-to-host layer and providing the link to the end user. This section briefly discusses some of the networking functions and protocols that operate at this level.

a) Monitoring Tools: SNMP

SNMP (Simple Network Management Protocol) is a protocol within the IP suite that manages network events and monitors the overall health of a network [10]. Events such as link failure, router failure, or anything causing loss of connectivity are reported to the network administrator. Monitoring the volume of traffic on a link is one way to manage events.

SNMP facilitates the evaluation of network health. Any device that uses TCP/IP can be managed using this protocol. SNMP communication occurs between network devices and management stations, which display the information for the administrator.

The network devices are commonly referred to as agents. Numerous variables are configured on the agents to provide tailored information about the overall network.

b) Assigning Addresses with DHCP

Dynamic Host Configuration Protocol (DHCP) is a server-based application that dynamically assigns IP addresses to network devices. This application eliminates at least two difficulties for a network administrator. First, it eliminates the need to statically address all the network devices. A static method implies constant updating as devices are moved within the network or even between networks. (For example, when there is a meeting between employees from different buildings and all employees bring laptops because they need to exchange data during the meeting, the laptops will require IP addresses) The second difficulty that DHCP eliminates is keeping track of a dynamic network with static addressing.

DHCP maintains a database of all addresses and to what device they are assigned, as well as which addresses are available. When a device running TCP/IP is initially logging on to the network, it sends out a DHCP discover message. The DHCP server receives the message and sends a message to the hardware or MAC address of the device, containing an IP address with the subnet mask, the time limit on the address lease, and IP address of the server. The device broadcasts a message of acceptance. The final step occurs when the address is actually assigned and the device implements its new identity. Once the process is complete, the device is capable of having TCP/IP sessions, and it operates as though the address were a permanent configuration. Once the address lease period expires, it is put back into the pool of addresses and becomes available for reallocation.

Another benefit of using DHCP is that there can be more users than addresses due to the fact that the addresses are leased for a limited amount of time. This would be appropriate if some network users did not frequently communicate with other services and

devices, such as e-mail and the Internet. Setting the ratio of users to addresses is a judgment call on the part of the administrator.

• Static NAT

c) Conserving with Network Address Translation

• Overloading (PAT)

Network address translation (NAT) is a method of IP address conservation. It is apparent that in any network, addresses are rapidly being depleted. This depletion is due to the fact that resources on the Internet are being used by far more people than initially expected. The way that the address space has been divided into classes is not optimized for the current and ever-growing number of users. VLSM is an attempt to alleviate some of the impact of wasted address space, but it is not a long-term solution. Using NAT in addition to VLSM is a way to extend the life (in terms of the address space) of the current version of IPv4. Development of a new version, IPv6, is under way and should theoretically combat the problematic shortage of address space. However, in the meantime, measures such as NAT are a good intermediate solution.

is assigned to a particular network making up the address pool. A new name is selected for

NAT gives networks that have private addresses the ability to access public networks (that is, the Internet). Typically, networks that have private addressing schemes, usually referred to as internal networks, are designed that way because a majority of the traffic on that network is local traffic, meaning that it does not leave the network. However, when a user needs access to the Internet, NAT translates the private address into a unique, public address. The public address comes from a pool of addresses reserved for that particular network. The number of addresses in the pool depends on the number of network users and the way NAT is configured.

The specifications and desired version of NAT are typically configured on a router. The router is responsible for the actual translation or mapping of internal and external addresses. In addition to address conservation, another benefit of NAT is security. The router configured with NAT enables anonymity. The external environment does not know the real identity of the user in the private network.

There are three types of NAT:

- Static NAT
- Dynamic NAT
- Overloading (PAT)

Static NAT refers to a configuration in which individual private addresses are assigned their own public addresses. This is useful when a limited number of users on the network frequently need to send and receive traffic outside the internal network. This configuration is not optimized when numerous users sporadically use the resources of an external network.

Dynamic NAT is a better-suited solution for numerous, sporadic external network users. This form of NAT operates by mapping an internal address with an address from an external address pool. Address mapping is illustrated in Figure 2.4. A unique address range is assigned to a particular network making up the address pool. As the name indicates, the process of mapping addresses is dynamic. Once a user is finished using the external address, the address enters into the pool and is available again.

Overloading, or port address translation (PAT), extends the functionality of dynamic NAT. This configuration is the most effective method of address conservation. PAT operates by mapping one external address to many internal addresses. To an external network, the users on the internal network appear as one user as illustrated in figure 2.4.

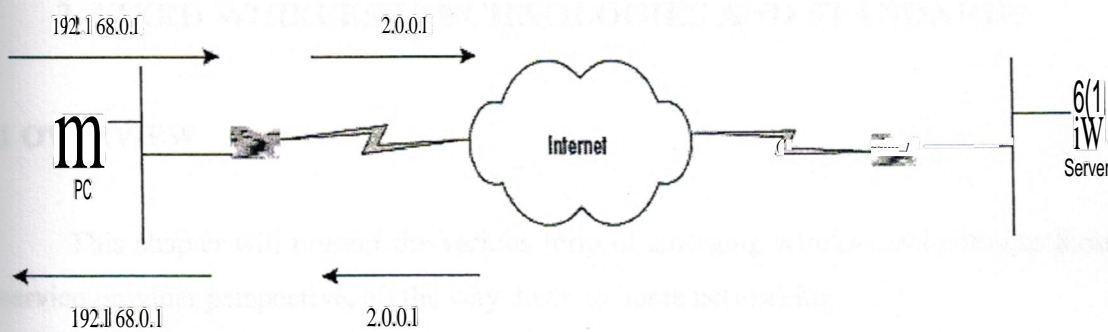


Figure 2.4 Network Address Translation [11]

The external network does not care, since the single address for the internal network is indeed unique, and that is all that matters.

2.9 SUMMARY

With the explosion of the internet, the internet protocol (IP) is the protocol is perhaps the most important protocol to come across any surface. When an IP based network is about to lay down and installed, it is necessary to have a full knowledge of Transmission Control Protocol (TCP/IP), and how it relates to the open conventions of the OSI (Open System Interconnection) Reference Model.

3. FIXED WIRELESS TECHNOLOGIES AND STANDARDS

3.1 OVERVIEW

This chapter will present the various form of emerging wireless technologies from a service provider perspective, all the way down to home networking.

3.2 MULTI CHANNEL MULTIPOINT DISTRIBUTION SERVICE

Allocated by the Federal Communications Commission (FCC) in 1983 and enhanced with two-way capabilities in 1998, Multichannel Multipoint Distribution Service (MMDS) is a licensed spectrum technology operating in the 2.5 to 2.7 GHz range, giving it 200 MHz of spectrum to construct cell clusters [12]. Service providers consider MMDS a complementary technology to their existing digital subscriber line (DSL) and cable modem offerings by providing access to customers not reachable via these wireline technologies shown in figure 3.1.

Figure 3.1 MMDS Architecture [13]

MMDS provides from 1 to 2 Mbps of throughput and has a cell size of 10 to 20 km. It is a radio-based technology (RPT) based on spread spectrum technology. It requires a clear line of sight between the radio (RPT) and the subscriber. Although several vendors are working on MMDS offerings that don't require a clear line of sight, the first of these offerings is still in the early stages of development. The use of reflective surfaces to direct the signal path can be used to overcome the lack of a clear line of sight. This is done by reflecting the signal off of a surface that is visible to both the radio and the subscriber. This is done by reflecting the signal off of a surface that is visible to both the radio and the subscriber. This is done by reflecting the signal off of a surface that is visible to both the radio and the subscriber.

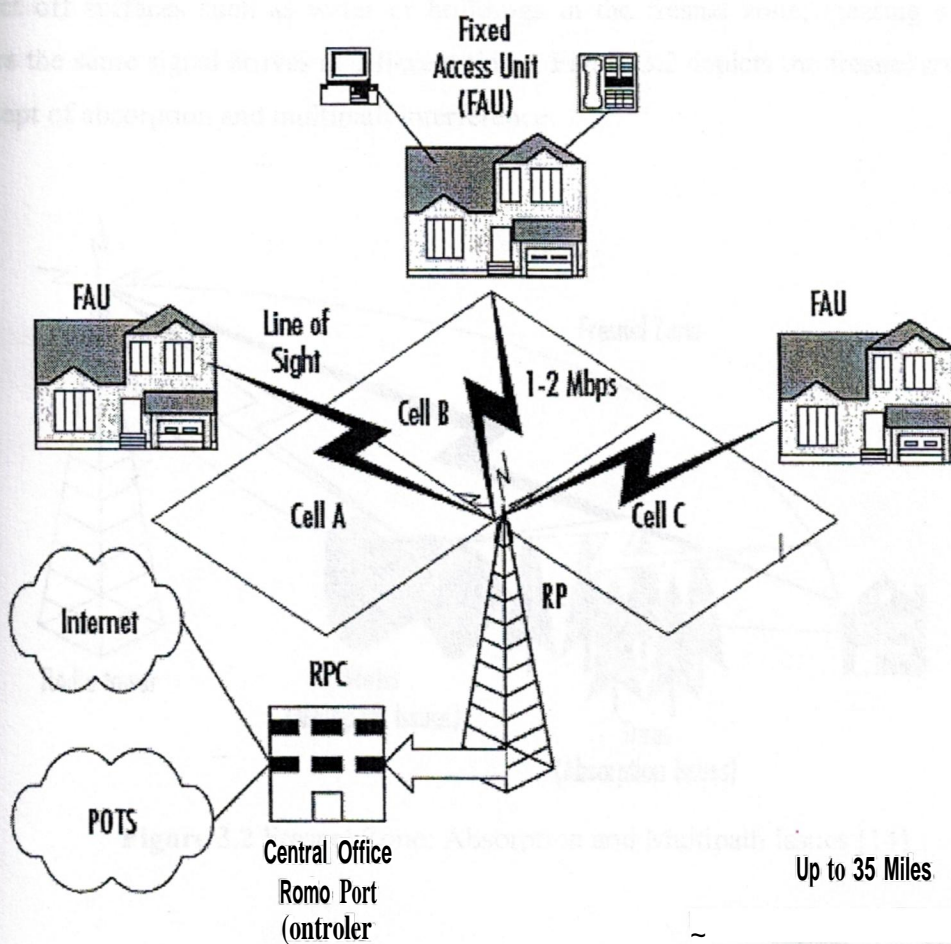


Figure 3.1 MlvIDS Architecture [13]

MMDS provides from 1 to 2 Mbps of throughput and has a relative range of 35 miles from the radio port controller (RPC) based on signal power levels. It generally requires a clear line of sight between the radio port (RP) antenna and the customer premise antenna, although several vendors are working on MMDS offerings that don't require a clear line of sight. The Fresnel zone of the signal (the zone around the signal path that must be clear of reflective surfaces) must be clear from obstruction as to avoid absorption and reduction of the signal energy. MlvIDS is also susceptible to a condition known as *multipath* reflection. Multipath reflection or interference happens when radio signals

reflect off surfaces such as water or buildings in the fresnel zone, creating a condition where the same signal arrives at different times. Figure 3.2 depicts the fresnel zone and the concept of absorption and multipath interference.

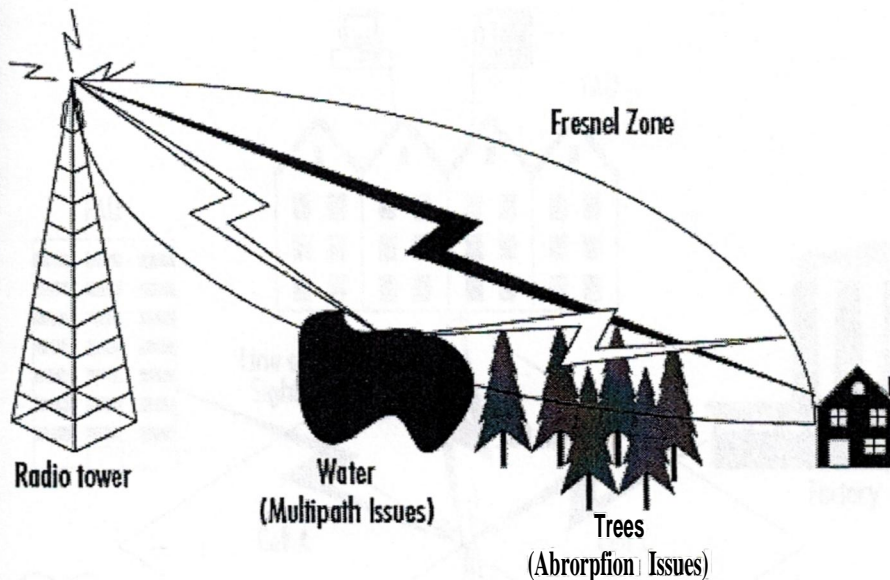


Figure 3.2 Fresnel Zone: Absorption and Multipath Issues [14]

3.3 LOCAL MULTIPOINT DISTRIBUTION SERVICE

Local Multipoint Distribution Service (LMDS) is a broadband wireless point-to-multipoint microwave communication system operating above 20 GHz (28-38 GHz). It is similar in its architecture to MMDS with a couple of exceptions. LMDS provides very high-speed bandwidth (upwards of 500 Mbps) but is currently limited to a relative maximum range of 3 to 5 miles of coverage. It has the same line-of-sight issues that MMDS experiences, and can be affected by weather conditions, as is common among line-of-sight technologies.

LMDS is ideal for short-range campus environments requiring large amounts of bandwidth, or highly concentrated urban centers with large data/voice/video bandwidth

requirements in a relatively small area. LMDS provides a complementary wireless architecture for the wireless service providers to use for markets that are not suited for $\sim S$ deployments. Figure 3.3 illustrates a generic LMDS architecture.

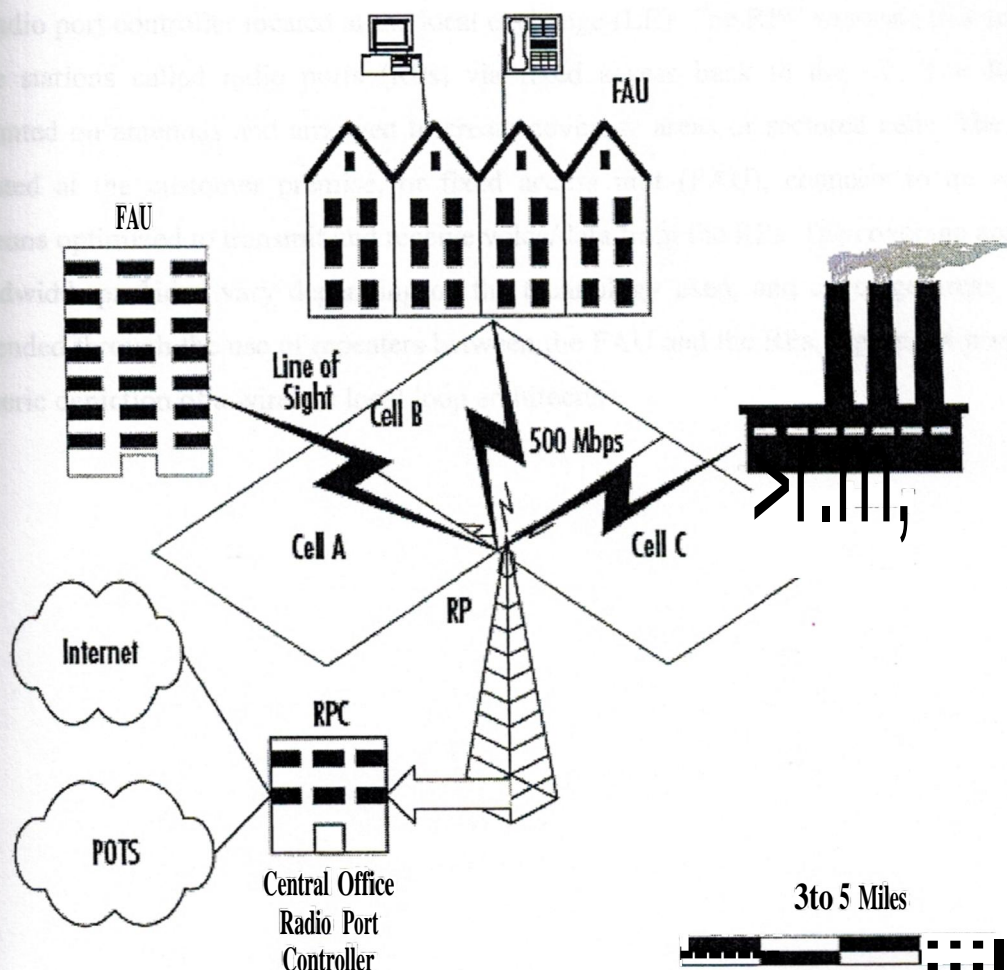


Figure 3.3 Local Multipoint Distribution Services (LMDS) Architecture [15]

3.4 WIRELESS LOCAL LOOP

Wireless Local Loop (WLL) refers to a fixed wireless class of technology aimed at providing last-mile services normally provided by the local service provider over a

wireless medium. This includes Plain Old Telephone Service (POTS) as well as broadband offerings such as DSL service.

The generic layout involves a point-to-multipoint architecture with a central radio or radio port controller located at the local exchange (LE). The RPC connects to a series of base stations called radio ports (RPs) via fixed access back to the LE. The RPs are mounted on antennas and arranged to create coverage areas or sectorized cells. The radios located at the customer premise, or fixed access unit (FAU), connects to an external antenna optimized to transmit and receive voice/data from the RPs. The coverage areas and bandwidth provided vary depending on the technology used, and coverage areas can be extended through the use of repeaters between the FAU and the RPs. Figure 3.4 provides a generic depiction of a wireless local loop architecture.

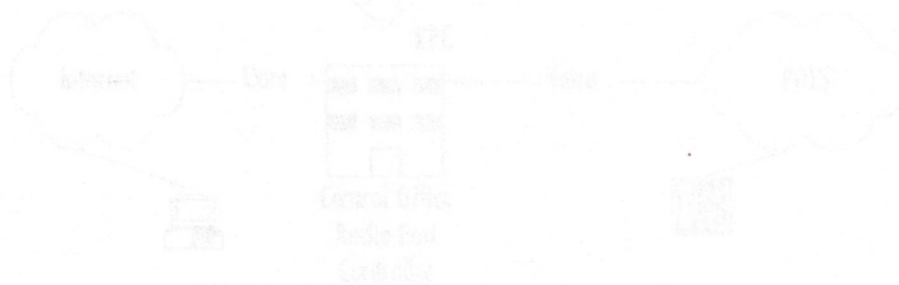


Figure 3.4 Wireless Local Loop Architecture [16]

3.5 POINT-TO-POINT MICROWAVE

Point-to-Point Microwave (PTP) is a line-of-sight technology, which is affected by multipath and absorption from dry woods and land. PTP Microwave falls into two categories: licensed and unlicensed, or spread spectrum. The FCC issues licenses for individuals to use specific frequencies for the licensed version. The advantage with the licensed PTP Microwave is that the chance of interference or noise sources in the frequency range is reduced. But, it comes at the high price of the carrier to that link needs to

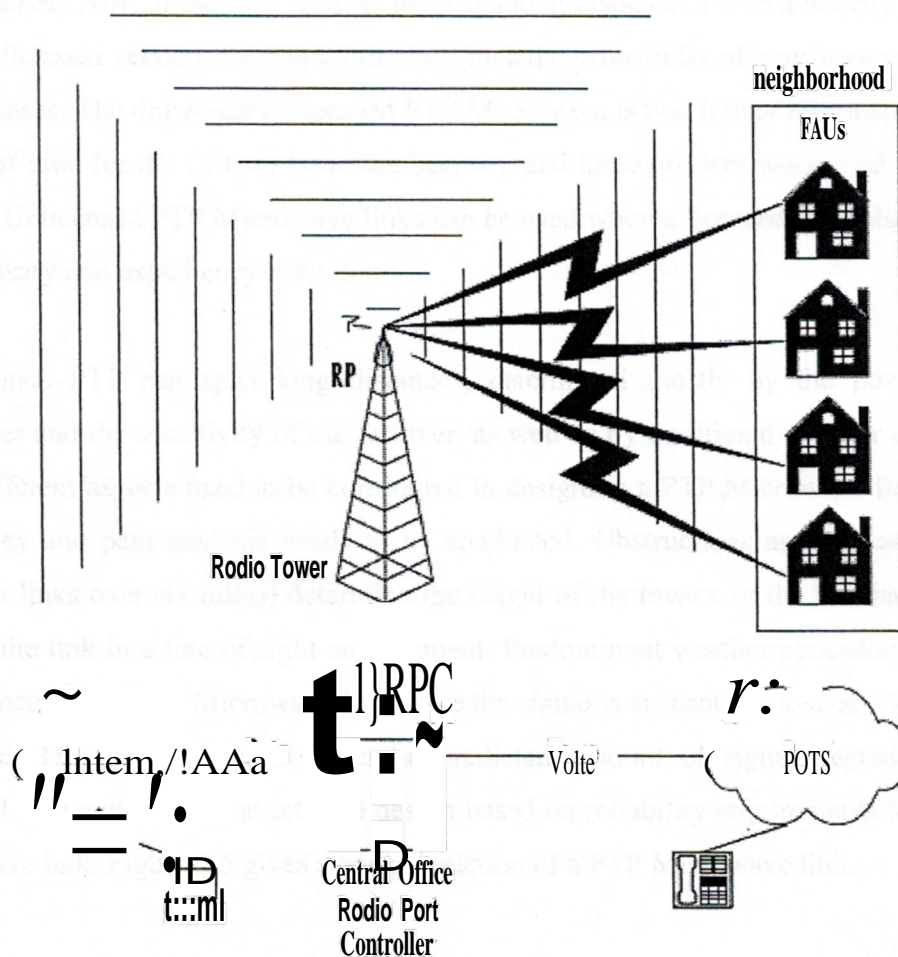


Figure 3.4 Wireless Local Loop Architecture [16]

3.5 POINT-TO-POINT MICROWAVE

Point-to-Point Microwave (PTP) is a line-of-sight technology, which is affected by multipath and absorption much like MMDS and LMDS. PTP Microwave falls into two categories: licensed and unlicensed, or spread spectrum. The FCC issues licenses for individuals to use specific frequencies for the licensed version. The advantage with the licensed PTP Microwave is that the chance of interference or noise sources in the frequency range is remote. This is critical if the integrity of the traffic on that link needs to

be maintained. Also, if the link is going to span a long distance or is in a heavily populated area, the licensed version is a much safer bet since the probability of interference is greater in those cases. The drawback to licensed PTP Microwave is that it may take a considerable amount of time for the FCC to issue the licenses, and there are fees associated with those licenses. Unlicensed PTP Microwave links can be used when a licensed PTP Microwave is not necessary and expediency is an issue.

Since PTP can span long distances, determined mostly by the power of the transmitter and the sensitivity of the receiver, as well as by traditional weather conditions, many different aspects need to be considered in designing a PTP Microwave link. First, a site survey and path analysis needs to be conducted. Obstructions and curvature of the earth (for links over six miles) determine the height of the towers or the building required to build the link in a line-of-sight environment. Predominant weather conditions can limit the distance of the PTP Microwave link since the signal is susceptible to a condition called rain fade. The designers must take the predicted amount of signal degradation in a projected area and factor that into the design based on reliability requirements for the PTP Microwave link. Figure 3.5 gives a basic depiction of a PTP Microwave link.

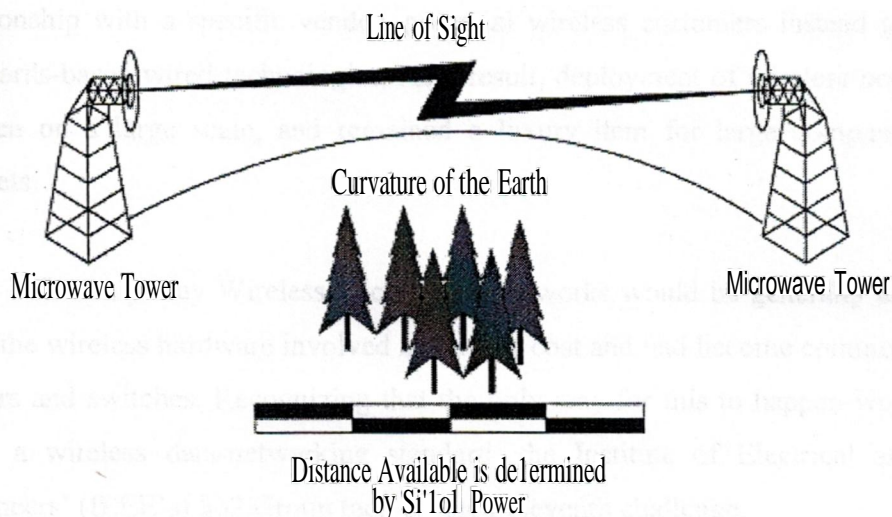


Figure 3.5 Point-to-Point Microwave [17]

3.6 WIRELESS LOCAL AREA NETWORKS

Benefits of fixed wireless can also provide value to the enterprise and home networks. This is where wireless capabilities get exciting for the end user. The benefits are literally at the fingertips. Imagining sitting at a desk when the boss calls announcing an emergency meeting immediately-there is a document on its way to us via e-mail that will be the focus of the meeting. Before wireless, first one would have to wait for the computer to receive the e-mail, then perhaps print the document before traveling to the meeting; with a laptop, cords, batteries, and connections. After the meeting, one would go back to his desk for any document changes or further correspondence by e-mail. In a wireless environment, the e-mail is received and the document is read while on the way to the meeting, and changes are made to the document and corresponded with other attendees real-time during the meeting.

3.7 NEED FOR A WIRELESS LAN STANDARD

Prior to the adoption of the 802.11 standard, wireless data-networking vendors made equipment that was based on proprietary technology. Wary of being locked into a relationship with a specific vendor, potential wireless customers instead turned to more standards-based wired technologies. As a result, deployment of wireless networks did not happen on a large scale, and remained a luxury item for large companies with large budgets.

The only way Wireless Local Area Networks would be generally accepted would be if the wireless hardware involved had a low cost and had become commodity items like routers and switches. Recognizing that the only way for this to happen would be if there were a wireless data-networking standard, the Institute of Electrical and Electronics Engineers' (IEEE's) 802 Group took on their eleventh challenge.

Since many of the members of the 802.11 Working Group were employees of vendors making wireless technologies, there were many pushes to include certain functions in the final specification. Although this slowed down the progress of finalizing 802.11, it also provided momentum for delivery of a feature-rich standard left open for future expansion.

On June 26, 1997, the IEEE announced the ratification of the 802.11 standard for wireless local area networks. Since that time, costs associated with deploying an 802.11-based network have dropped, and WLANs rapidly are being deployed in schools, businesses, and homes [18].

3.7.1 Definition of 802.11 Standards

As in all 802.x standards, the 802.11 specification covers the operation of the media access control (MAC) and physical layers. As seen in Figure 3.6, 802.11 define a MAC sublayer, MAC services and protocols, and three physical (PHY) layers.

Data-Link Layer	802.2		
	802.11 MAC		
Physical Layer	FHSS	DSSS	IR

Figure 3.6 802.11 Frame Format

The three physical layer options for 802.11 are infrared (IR) baseband PHY and two radio frequencies (RF) PHYs. Due to line-of-sight limitations, very little development has occurred with the Infrared PHY.

The RF physical layer is composed of Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) in the 2.4 GHz band. All three physical layers operate at either 1 or 2 Mbps. The majority of 802.11 implementations utilize the DSSS method.

FHSS works by sending bursts of data over numerous frequencies. As the name implies, it hops between frequencies. Typically, the devices use up to four frequencies simultaneously to send information and only for a short period of time before hopping to new frequencies. The devices using FHSS agree upon the frequencies being used. In fact, due to the short time period of frequency use and device agreement of these frequencies, many autonomous networks can coexist in the same physical space.

DSSS functions by dividing the data into several pieces and simultaneously sending the pieces on as many different frequencies as possible, unlike FHSS, which sends on a limited number of frequencies. This process allows for greater transmission rates than FHSS, but is vulnerable to greater occurrences of interference. This is because the data is spanning a larger portion of the spectrum at any given time than FHSS. In essence, DSSS floods the spectrum all at one time, whereas FHSS selectively transmits over certain frequencies.

3.7.2 Guaranteeing Compatibility

As mentioned earlier, the primary reason WLANs were not widely accepted was the lack of standardization. It is logical to question whether vendors would accept a nonproprietary operating standard, since vendors compete to make unique and distinguishing products. Although 802.11 standardized the PHY, MAC, the frequencies to send/receive on, transmission rates and more, it did not absolutely guarantee that differing vendors' products would be 100 percent compatible. In fact, some vendors built in backward-compatibility features into their 802.11 products in order to support their legacy customers. Other vendors have introduced proprietary extensions (for example, bit-rate

adaptation and stronger encryption) to their 802.11 offerings. To ensure that consumers can build interoperating 802.11 wireless networks, an organization called the Wireless Ethernet Compatibility Alliance (WECA) tests and certifies 802.11 devices.

Their symbol of approval means that the consumer can be assured that the particular device has passed a thorough test of interoperations with devices from other vendors. This is important when considering devices to be implemented into an existing network, because if the devices cannot communicate, it complicates the management of the network—in fact, essentially two autonomous networks would have to be dealt with. It is also important when building a new network because it may be limited to a single vendor.

Since the first 802.11 standard was approved in 1997, there have been several initiatives to make improvements. As observed in the following sections, there is an evolution unfolding with the 802.11 standard [19].

The introduction of the standard came with 802.11 followed by 802.11b. Then along came 802.11a, which provides up to five times the bandwidth capacity of 802.11b [20]. Now, accompanying the ever-growing demand for multimedia services is the development of 802.11e. Each task group, outlined next, is endeavoring to speed up the 802.11 standard, making it globally accessible, while not having to reinvent the MAC layer of 802.11:

- **The 802.11d Working Group** is concentrating on the development of 802.11 WLAN equipment to operate in markets not served by the current standard (the current 802.11 standard defines WLAN operation in only a few countries).
- **The 802.11f Working Group** is developing an Inter-Access Point Protocol, due to the current limitation prohibiting roaming between access points made by different vendors. This protocol would allow wireless devices to roam across access points made by competing vendors.

- The 802.11g Working Group is working on furthering higher data rates in the 2.4GHz radio band.
- The 802.11h Working Group is busy developing Spectrum and Power Management Extensions for the IEEE 802.11a standard for use in Europe.802.11b Ignoring the FHSS and IR physical mediums, the 802.11b PHY uses DSSS to broadcast in any one of 14 center-frequency channels in the 2.4 GHz Industrial, Scientific, and Medical (ISM) radio band. As Table 3.1 shows, North America allows 11 channels; Europe allows 13, the most channels allowed. Japan has only one channel reserved for 802.11, at 2.483 GHz.

Table 3.1 802.11b Channels and Participating Countries

Channel Number	Frequency GHz	North America	Europe	Spain	France	Japan
1	2.412	X	X			
2	2.417	X	X			
3	2.422	X	X			
4	2.427	X	X			
5	2.432	X	X			
6	2.437	X	X			
7	2.442	X	X			
8	2.447	X	X			
9	2.452	X	X			
10	2.457	X	X	X	X	
11	2.462	X	X	X	X	
12	2.467		X		X	
13	2.472		X		X	
14	2.483					X

There are many different devices competing for airspace in the 2.4 GHz radio spectrum. Unfortunately, most of the devices that cause interference are especially common in the home environment, such as microwaves and cordless phones. As imagined, the viability of an 802.11b network depends on how many of these products are near the network devices.

One of the more recent entrants to the 802.11b airspace comes in the form of the emerging Bluetooth wireless standard. Though designed for short-range transmissions, Bluetooth devices utilize FHSS to communicate with each other. Cycling through thousands of frequencies a second, this looks as if it poses the greatest chance of creating interference for 802.11. Further research will determine exactly what-if any interference Bluetooth will cause to 802.11b networks. Many companies are concerned with over saturating the 2.4 GHz spectrum, and are taking steps to ensure that their devices "play nicely" with others in this arena. These forms of interference will directly impact the home user who wishes to set up a wireless LAN, especially if neighbors operate interfering devices. Only time will tell if 802.11b will be able to stand up against these adversaries and hold on to the marketplace.

3.8 802.11a Standard

Due to the overwhelming demand for more bandwidth and the growing number of technologies operating in the 2.4 GHz band, the 802.11a standard was created for WLAN use in North America as an upgrade from the 802.11b standard. 802.11a provides 25 to 54 Mbps bandwidth in the 5 GHz spectrum (the unlicensed national information infrastructure [U-NII] spectrum). Since the 5 GHz band is currently mostly clear, chance of interference is reduced [21]. However, that could change since it is still an unlicensed portion of the spectrum. 802.11a still is designed mainly for the enterprise, providing Ethernet capability. 802.11a is one of the physical layer extensions to the 802.11 standard.

Abandoning spread spectrum completely, 802.11a uses an encoding technique called Orthogonal Frequency Division Multiplexing (OFDM). Although this encoding technique is similar to the European 5-GHz HiperLAN physical layer specification.

As shown in Table 3.2, three 5-GHz spectrums have been defined for use with 802.11a. Each of these three center-frequency bands covers 100 MHz.

Table 3.2 802.11a Channels Usable in the 5-GHz U-NII Radio Spectrum

Regulatory Area	Frequency Band	Channel Number	Centre Frequencies
USA	U-NII Lower Band 5.15 -5.25 GHz	36	5.180 GHz
		40	5.200 GHz
		44	5.220 GHz
		48	5.240 GHz
USA	U-NII Middle Band 5.25 -5.35 GHz	52	5.260 GHz
		56	5.280 GHz
		60	5.300 GHz
		64	5.320 GHz
USA	U-NII Upper Band 5.725-5.825 GHz	149	5.745 GHz
		153	5.765 GHz
		157	5.785 GHz
		161	5.805 GHz

The IEEE 802.11e is providing enhancements to the 802.11 standard while retaining compatibility with 802.11b and 802.11a. The enhancements include multimedia capability made possible with the adoption of quality of service (QoS) functionality as well as security improvements.

QoS is the key to the added functionality with 802.11e. It provides the functionality required to accommodate time-sensitive applications such as video and audio. QoS includes queuing, traffic shaping tools, and scheduling. These characteristics allow priority of traffic. For example, data traffic is not time sensitive and therefore has a lower priority than applications like streaming video.

3.9 DEVELOPING WLANS THROUGH THE 802.11 ARCHITECTURE

The 802.11 architecture can best be described as a series of interconnected cells, and consists of the following: the wireless device or station, the access point (AP), the wireless medium, the distribution system (DS), the basic service set (BSS), the extended service set (ESS), and station and distribution services. All of these working together providing a seamless mesh give wireless devices the ability to roam around the WLAN looking for all intents and purposes like a wired device.

3.9.1 The Basic Service Set

The core of the IEEE 802.11 standard is the basic service set (BSS). This model is made up of one or more wireless devices communicating with a single Access Point (AP) in a single radio cell. If there are no connections back to a wired network, this is called an independent basic service set as shown in figure 3.7.

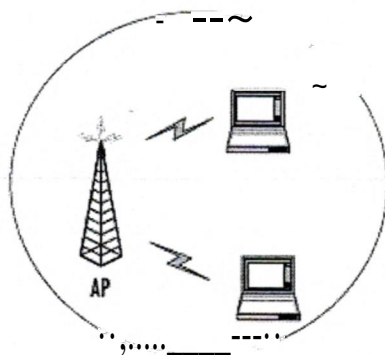


Figure 3.7 Basic Service Set [22]

If there is no access point in the wireless network, it is referred to as an ad-hoc network. This means that all wireless communications is transmitted directly between the members of the ad-hoc network. Figure 3.8 describes a basic ad-hoc network.

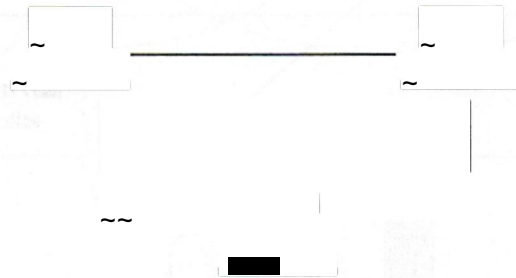


Figure 3.8 Ad-Hoc Network

When the BSS has a connection to the wired network via an AP, it is called an infrastructure BSS. The model is shown in Figure 3.9; the AP bridges the gap between the wireless device and the wired network.

3.9.2 The Extended Service Set

The compelling force behind WLAN deployment at the 802.11b and 802.11g users are free to move about without having to worry about connecting to various networks manually. If operating with a single infrastructure BSS, the operating area would be limited to the signal range of the AP. Through the extended service set (ESS), the IEEE 802.11 architecture allows users to move between multiple infrastructure BSSs. In an ESS, the APs talk among themselves to forwardly traffic from one BSS to another, as well as switch the roaming devices from one BSS to another. They do this using a medium called the distribution system (DS). The distribution system forms the spine of the WLAN.

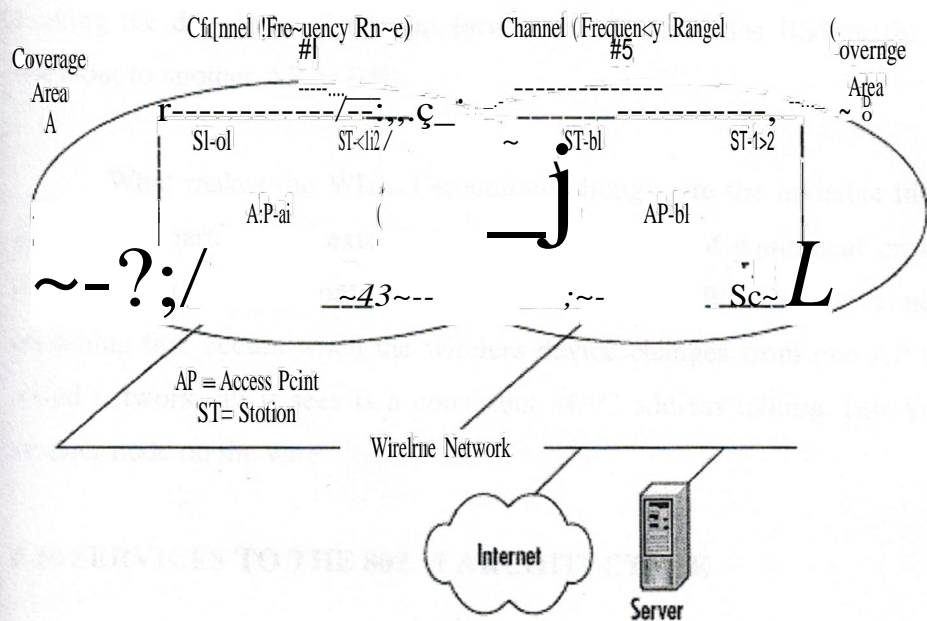


Figure 3.9 the 802.11 infrastructure architecture

Since multiple Access Points exist in this model, the wireless devices no longer communicate in a peer-to-peer fashion. Instead, all traffic from one device destined for another device is relayed through the AP. Even though it would look like this would double the amount of traffic on the WLAN, this also provides for traffic buffering on the AP when a device is operating in a low-power mode.

3.9.2 The Extended Service Set

The compelling force behind WLAN deployment is the fact that with 802.11, users are free to move about without having to worry about switching network connections manually. If operating with a single infrastructure BSS, this moving about would be limited to the signal range of the AP. Through the extended service set (ESS), the IEEE 802.11 architecture allows users to move between multiple infrastructure BSSs. In an ESS, the APs talk amongst themselves forwarding traffic from one BSS to another, as well as switch the roaming devices from one BSS to another. They do this using a medium called the distribution system (DS). The distribution system forms the spine of the WLAN,

making the decisions whether to forward traffic from one BSS to the wired network or back out to another AP or BSS.

What makes the WLAN so unique, though, are the invisible interactions between the various parts of the extended service set. Pieces of equipment on the wired network have no idea they are communicating with a mobile WLAN device, nor do they see the switching that occurs when the wireless device changes from one AP to another. To the wired network, all it sees is a consistent MAC address talking, just as if the MAC was another node on the wire.

3.10 SERVICES TO THE 802.11 ARCHITECTURE

There are nine different services that provide behind-the-scenes support to the 802.11 architecture. Of these nine, four belong to the station services group and the remaining five to the distribution services group.

a) Station Services

The four station services namely authentication, de-authentication, data delivery, and privacy, provide functionality equal to what standard 802.3 wired networks would have.

The authentication service defines the identity of the wireless device. Without this distinct identity, the device is not allowed access to the WLAN. Authentication can also be made against a list of MACs allowed to use the network. This list of allowable MAC addresses may be on the AP or on a database somewhere on the wired network. A wireless device can authenticate itself to more than one AP at a time. This sort of "pre-authentication" allows the device to prepare other APs for its entry into their airspace.

The de-authentication service is used to destroy a previously known station identity. Once the de-authentication service has been started, the wireless device can no longer access the WLAN. This service is invoked when a wireless device shuts down, or when it is roaming out of the range of the access point. This frees up resources on the AP for other devices. Just like its wired counterparts, the 802.11 standard specifies a data delivery service to ensure that data frames are transferred reliably from one MAC to another.

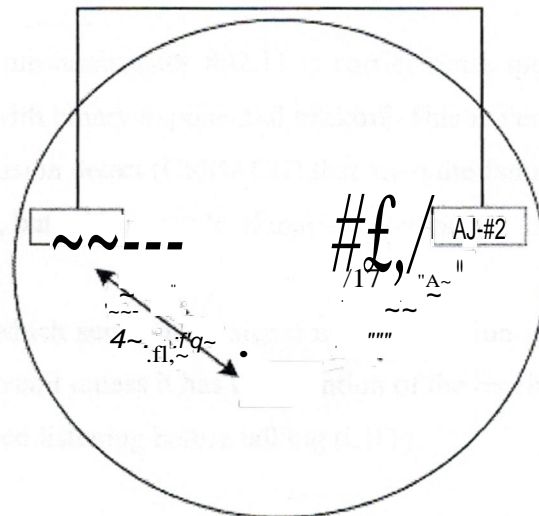
The privacy service is used to protect the data as it crosses the WLAN. Even though the service utilizes an RC4-based encryption scheme, it is not intended for end-to-end encryption or as a sole method of securing data. Its design was to provide a level of protection equivalent to that provided on a wired network-hence its moniker Wireless Equivalency Privacy (WEP).

b) Distribution Services

Between the Logical Link Control (LLC) sublayer and the MAC, five distribution services make the decisions as to where the 802.11 data frames should be sent. These distribution services make the roaming handoffs when the wireless device is in motion. The five services are association, re-association, disassociation, integration, and distribution.

The wireless device uses the association service as soon as it connects to an AP. This service establishes a logical connection between the devices, and determines the path the distribution system needs to take in order to reach the wireless device. If the wireless device does not have an association made with an access point, the DS will not know where that device is or how to get data frames to it. In Figure 3.9, the wireless device can be authenticated to more than one AP at a time, but it will never be associated with more than one AP. While dealing with roaming and low-power situations, sometimes the wireless device will not be linked continuously to the same AP. To keep from losing

whatever network session information the wireless device has, the re-association service is used. This service is similar to the association service, but includes current information about the wireless device. In the case of roaming, this information tells the current AP who the last AP was. This allows the current AP to contact the previous AP to pick up any data frames waiting for the wireless device and forward them to their destination.



This wireless device is authenticated to both Access Points, but its only association exists with AP #1.

Figure 3.10 Wireless Authentications through the Association Service [23].

The disassociation service is used to tear down the association between the AP and the wireless device. This could be because the device is roaming out of the AP's area, the AP is shutting down, or any one of a number of other reasons. To keep communicating to the network, the wireless device will have to use the association service to find a new AP.

The distribution service is used by APs when determining whether to send the data frame to another AP and possibly another wireless device, or if the frame is destined to head out of the WLAN into the wired network.

The integration service resides on the APs as well. This service does the data translation from the 802.11 frame format into the framing format of the wired network. It also does the reverse, taking data destined for the WLAN, and framing it within the 802.11 frame format.

3.11 THE CSMA-CA MECHANISM

The basic access mechanism for 802.11 is carrier sense multiple access collision avoidance (CSMA-CA) with binary exponential backoff. This is very similar to the carrier sense multiple access collision detect (CSMA/CD) that are quite familiar when dealing with standard 802.3 (Ethernet), but with a couple of major differences.

Unlike Ethernet, which sends out a signal until a collision is detected, CSMA-CA takes great care to not transmit unless it has the attention of the receiving unit, and no other unit is talking. This is called listening before talking (LBT).

Before a packet is transmitted, the wireless device *will* listen to hear if any other device is transmitting. *If a transmission is occurring, the device will wait for a randomly determined period of time, and then listen again. If no one else is using the medium, the device will begin transmitting. Otherwise, it will wait again for a random time before listening once more.*

3.12 THE RTS/CTS MECHANISM

To minimize the risk of the wireless device transmitting at the same time as another wireless device (and thus causing a collision), the designers of 802.11 employed a mechanism called Request To Send/Clear To Send (RTS/CTS).

For example, if data arrived at the AP destined for a wireless node, the AP would send a RTS frame to the wireless node requesting a certain amount of time to deliver data

to it. The wireless node would respond with a CTS frame saying that it would hold off any other communications until the AP was done sending the data. Other wireless nodes would hear the transaction taking place, and delay their transmissions for that period of time as well. In this manner, data is passed between nodes with a minimal possibility of a device causing a collision on the medium.

This also gets rid of a well-documented WLAN issue called the hidden node. In a network with multiple devices, the possibility exists that one wireless node might not know all the other nodes that are out on the WLAN. Thanks to RST/CTS, each node hears the requests to transmit data to the other nodes, and thus learns what other devices are operating in that BSS.

3.13 SUMMARY

This chapter provides an overview of differences and purposes of the emerging technologies in the wireless sector. The three primary areas of discussion are fixed wireless, mobile wireless, and optical wireless technology. The information in this chapter gives an understanding of which technology is the best solution for a specific network design.

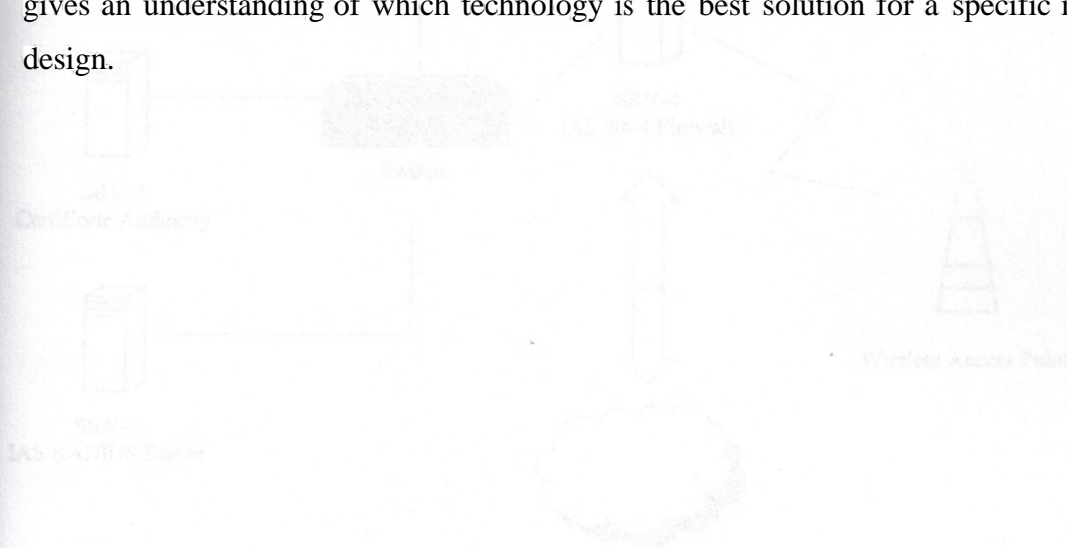


Figure 4.1 A review of the network and its necessary components for implementation

prepared by the author

4. AUTHENTICATION OF A WIRELESS NETWORK

4.1 OVERVIEW

In this chapter, a secure wireless network is developed using Protected Extensible Authentication Protocol (PEAP) and Microsoft Internet Security and Acceleration (ISA) Server 2004. A Certificate Authority will be implemented to issue certificates for authenticating the clients as well as the access points. Some prototypes of Wireless Access points will be configured accordingly. The Network will be tested and compared with another network without these security measures and results are shown.

4.2 OVERVIEW OF NETWORK CONFIGURATION

The wireless network illustrated as an example is shown in figure 4.1.

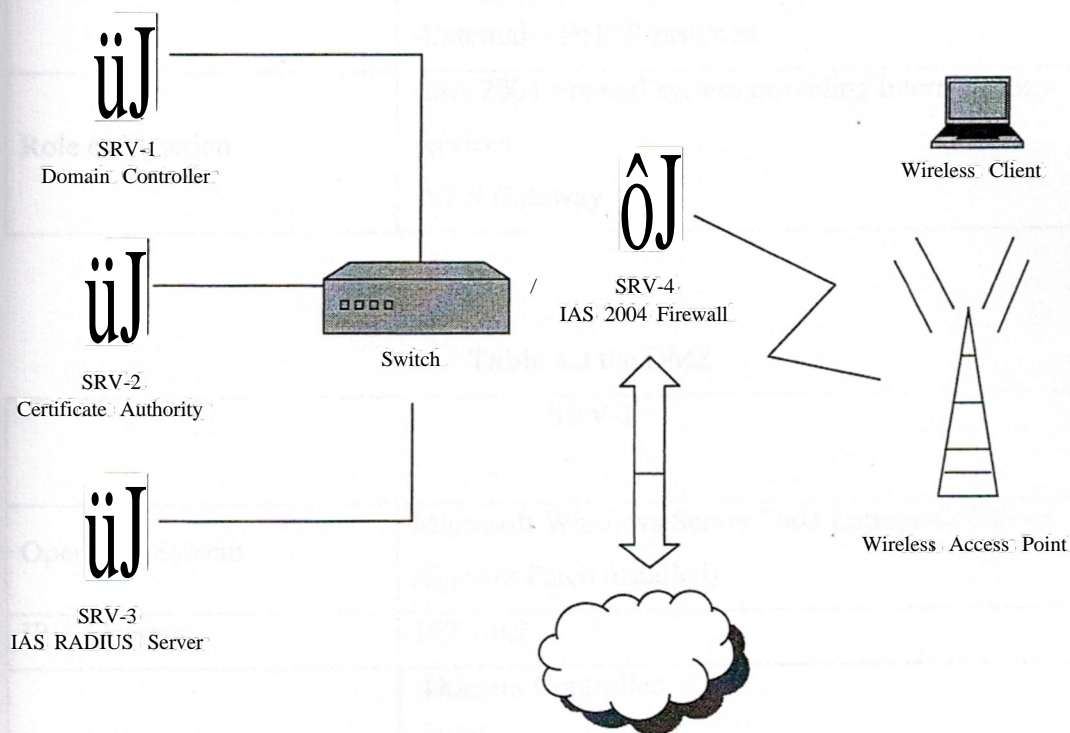


Figure 4.1 A layout of the network and the necessary components for authentication proposed by the author

Table 4.1 IP Address scheme

Segment	Subnet Address	Subnet Mask
Internal	172.1.0.0	255.255.0.0
Wireless Perimeter	192.168.1.0	255.255.255.0
External	DHCP assigned	DHCP assigned

Table 4.2 Gatekeeper configuration

SRV-4	
Operating System	Microsoft Windows Server 2003 Enterprise Edition (Current Patch installed)
IP Addresses	-Internal 172.1.0.1 -Wireless perimeter - 192.168.1.2 -External - DHCP assigned
Role or Function	-ISA 2004 firewall system providing internet proxy services -VPN Gateway

Table 4.3 the DMZ

SRV-1	
Operating System	Microsoft Windows Server 2003 Enterprise Edition (Current Patch installed)
IP Addresses	172.1.0.2
Role or Function	-Domain Controller -DNS -DHCP

SRV-2	
Operating System	Microsoft Windows Server 2003 Enterprise Edition (Current Patch installed)
IP Addresses	172.1.0.3
Role or Function	-Domain Controller -DNS -Certificate Authority
SRV-3	
Operating System	Microsoft Windows Server 2003 Enterprise Edition (Current Patch installed)
IP Addresses	172.1.0.4
Role or Function	IAS RADIUS Server

Table 4.1 and 4.2 shows how the IP addresses would be configured and their subnets and gives the specs for the gatekeeper for this network.

This type of network layout is referred to as a 3-leg perimeter network. The perimeter network in this case is the wireless network under consideration, however many people use this segment, also commonly referred to as the Demilitarized Zone (DMZ) in table 4.3, for their servers which publish services to the internet [24].

The reason for putting these publishing servers in their own network is because it is assumed that at some point they will be compromised because of flaws either in the operating systems themselves or in the components that comprise the services they provide to the internet. The wireless network is placed on its own segment to mitigate attacks of an entirely different nature. Wireless networks are inherently insecure and the flaws that exist in these networks are that of the actual transmission and encryption protocols and schemes,

something for which there are no patches for. While the argument can be made that since both networks have a high risk of compromise they could be isolated together in the same DMZ, it is recommended that there is no need to expand the attack surface of either network by combining the potential flaws, especially when all is required is an additional network card in the ISA server and a small switch or hub to connect all the access points. By establishing this perimeter network for the wireless to exist in, a sandbox of sorts for the users is created, and then access is granted into either the main network or onto the internet, or both, depending on the constraints the network administrators wish to impose. These access restrictions will come in the form of a dual factor authorization scheme followed by access restrictions placed on the user that authenticates. The first layer of defense will come from WPA RADIUS authentication which will grant users access to the wireless network itself. Once the wireless connection is established, a VPN tunnel will be created through the firewall and onto what ever network is chosen to let the given user have access to, giving a second line of defense. With this scenario, wireless traffic will flow through an encrypted tunnel wrapped inside another encrypted tunnel. By doing this, the network is multiple schemes. WPA could be broken completely, and this would still be a secure form of communication with the network [25].

4.3 PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL (PEAP)

● PEAP is an authentication protocol designed for wireless LANs. PEAP makes use of 2 well known and well studied protocols:

- 1. EAP - Extensible Authentication Protocol
- 2. TLS - Transport Layer Security

● EAP is an authentication protocol that typically rides on top of another protocol such as 802.1x, RADIUS, PPP, etc. EAP allows the authenticator to serve as the user authentication carrier between the client and the authentication server. EAP limitations are well known and resolved by PEAP.

TLS provides the encryption, compression and data integrity. TLS is based on the SSL 3.0 Protocol Specification and is often described as a improved version of SSL. TLS is well documented and has been extensively analyzed with no significant weaknesses found.

A wireless access point broadcasts all of its traffic so that anyone within broadcast range can passively collect the data. Wireless encryption is weak and can be decrypted in a short period of time using AirSnort or WEPCrack. Physical access of the network is not necessary to connect to the network. Knowledge of the SSID and possibly a valid MAC address is all that is required. Users have no way of knowing if they are connecting to a rogue access point setup as part of a man-in-the-middle attack.

PEAP uses the following ways to make the transmission secure shown in figure 4.2. Figure 4.3 and 4.4 reveal a thorough authentication scheme of a PEAP protocol.

- The transmission of user-sensitive authentication data is encrypted within a TLS tunnel.
- Data within the TLS tunnel cannot be decrypted without the TLS master secret.
- If a client does not successfully authenticate, its connection is dropped by the access point.
- The TLS master secret is not shared with the access point, so rogue access points will be unable to decrypt messages protected by PEAP.
- Server-side Public-Key Infrastructure (PKI) based digital certificates are used to authenticate EAP Servers.

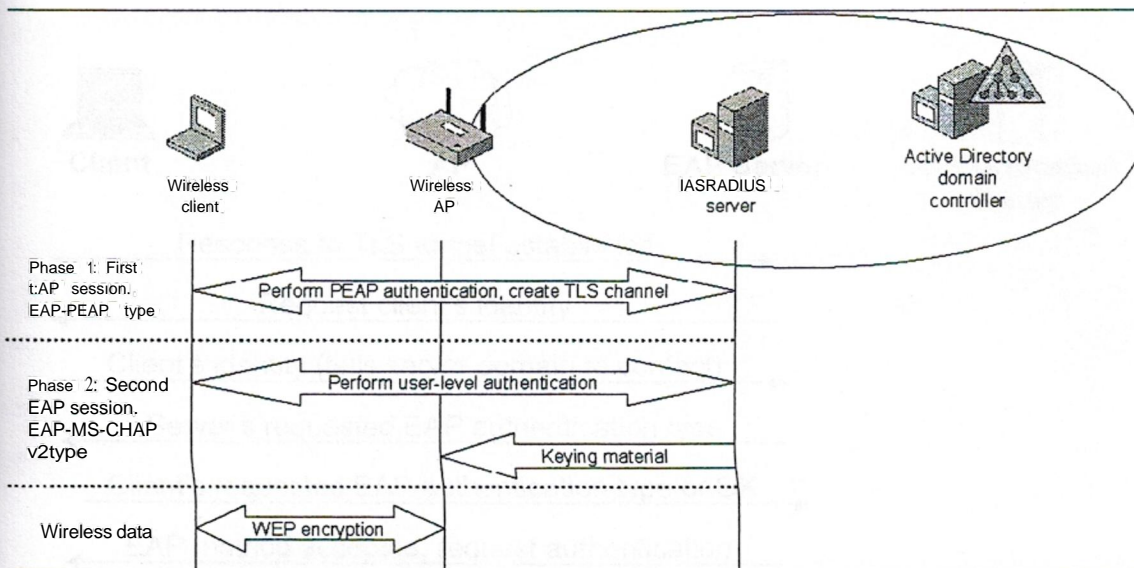


Figure 4.2 PEAP authentication scheme [26]

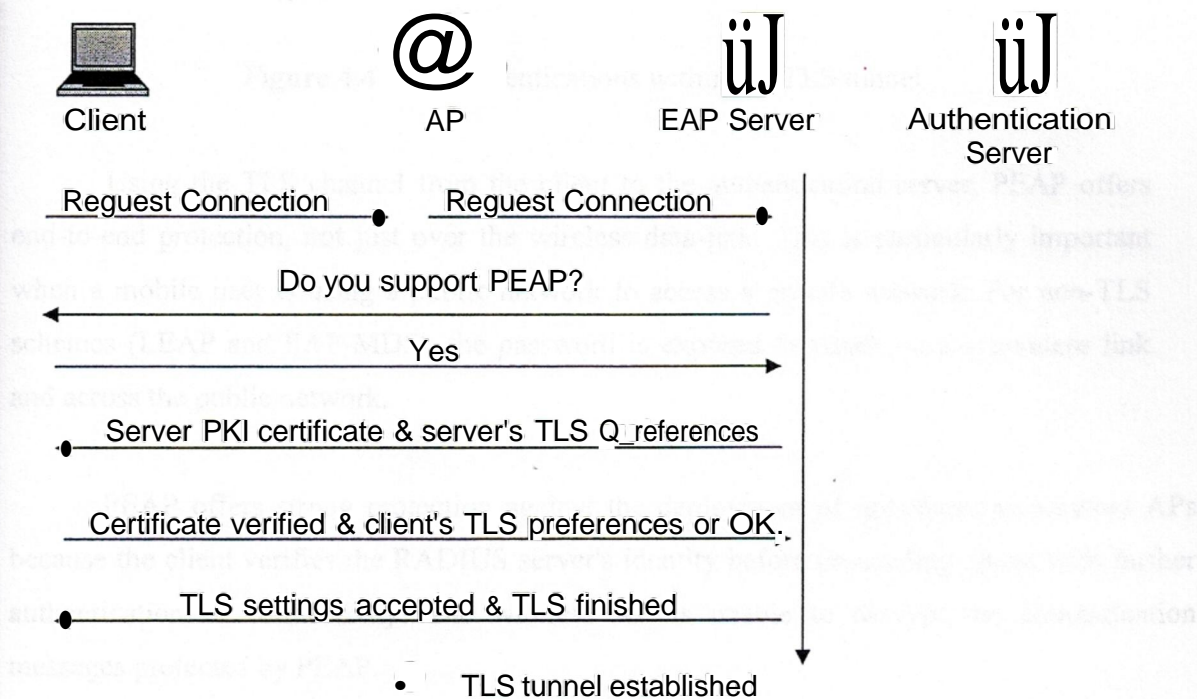


Figure 4.3 Establishing a TLS tunnel

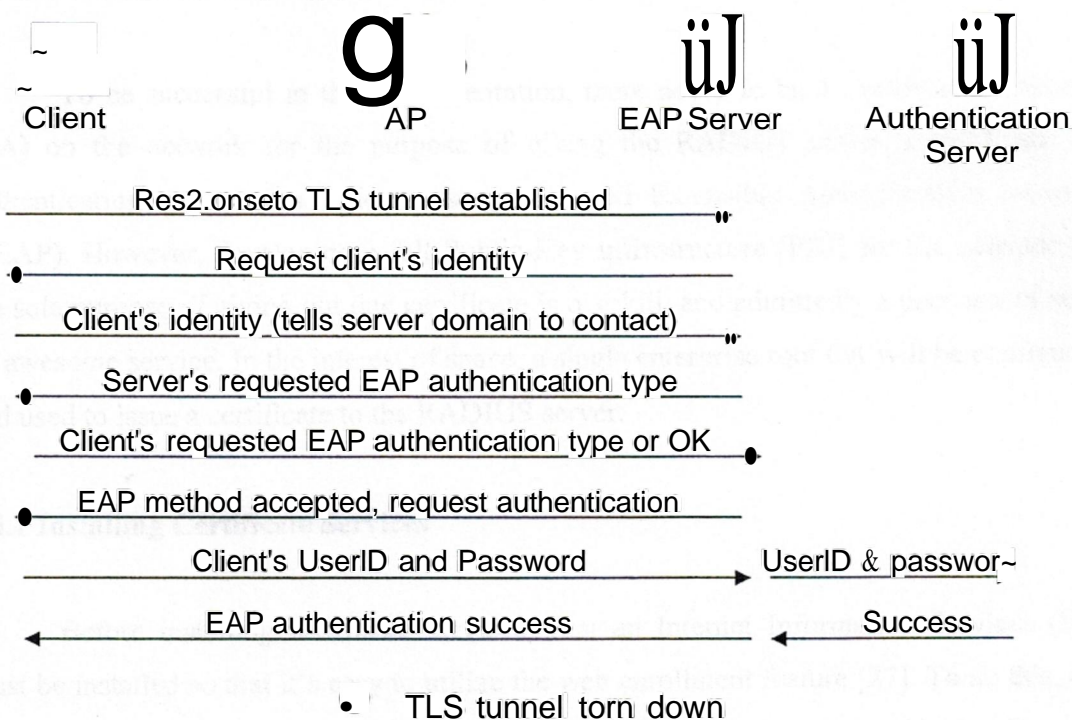


Figure 4.4 EAP authentications within the TLS tunnel

Using the TLS channel from the client to the authentication server, PEAP offers end-to-end protection, not just over the wireless data-link. This is particularly important when a mobile user is using a public network to access a private network. For non-TLS schemes (LEAP and EAP-MD5), the password is exposed to attack on the wireless link and across the public network.

PEAP offers strong protection against the deployment of unauthorized wireless APs because the client verifies the RADIUS server's identity before proceeding ahead with further authentication or connectivity. The wireless AP is unable to decrypt the authentication messages protected by PEAP.

4.4 INSTALLING AND CONFIGURING A CERTIFICATE AUTHORITY

To be successful in the implementation, there needs to be a Certificate Authority (CA) on the network for the purpose of giving the RADIUS server a certificate for authenticating the wireless clients using Protected Extensible Authentication Protocol (PEAP). However, developing a full Public-Key Infrastructure (PKI) for the network for the sole purpose of giving out one certificate is overkill, and admittedly a poor use of such an awesome service. In the interest of space, a single enterprise root CA will be configured and used to issue a certificate to the RADIUS server.

4.4.1 Installing Certificate Services

Before installing certificate services, first an Internet Information Services (IIS) must be installed so that it's easy to utilize the web enrollment feature [27]. To do this, the control panel on the server that needs to be CA is selected and the "Add / Remove Programs" clicked followed by clicking the "Add/Remove Windows Components" button. Next, the "Application Server" is double clicked from the list of available Windows Components and then "Internet Information Services (IIS)" is double clicked from the Application Server list. From the Internet Information Services window, double click "World Wide Web Service", and finally, a check is placed in the box next to "World Wide Web Service". Here "OK" in all the windows is clicked, and "Next" on the Windows Components Wizard is chosen. To conclude the installation of IIS, the "Finish" is clicked (Figure 4.5). Now the server is ready to have Certificate Services installed on it. From the "Add or Remove Programs" window, the "Add/Remove Windows Components" button is clicked again, and this time a check is put in the box beside "Certificate Services". A popup will appear letting us know that once the service is installed administrators cannot change the name or the domain membership of the system, simply click "Yes", and then "Next". For the purpose of this chapter, an Enterprise root CA is installed, which is done by clicking the radio button next to "Enterprise root CA", followed by clicking "Next".

The next step is to name the CA; for this network domain this will simply be "EnterpriseRoot" as shown in Figure 4.6.

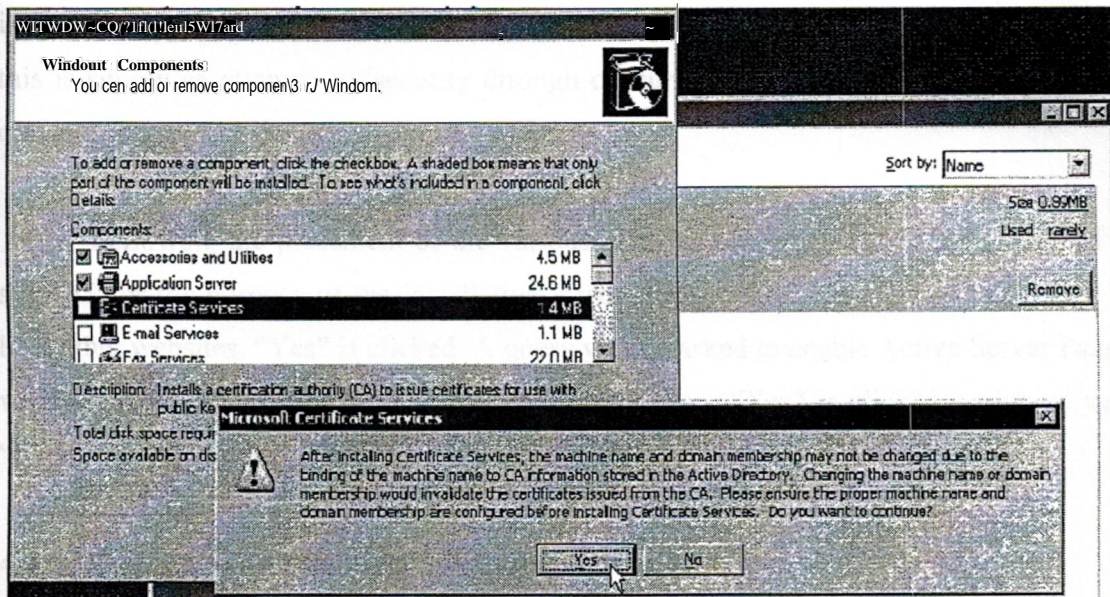


Figure 4.5 Installing IIS on a Microsoft Windows Server 2003 OS

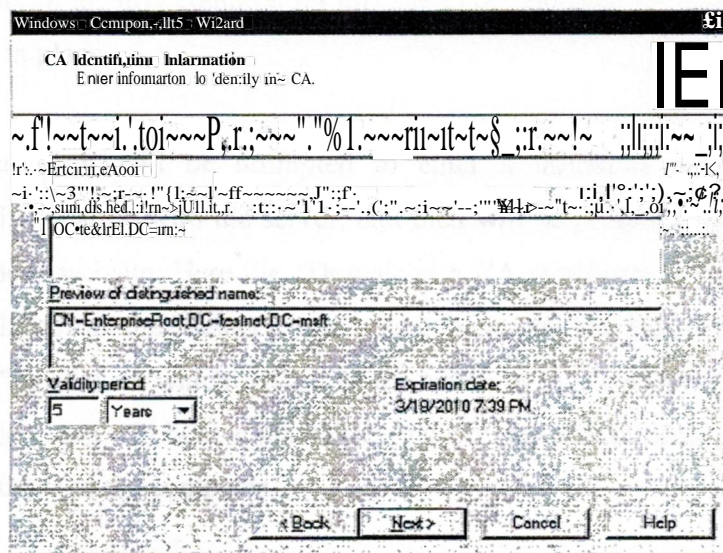


Figure 4.6 Installing a Certificate authority called enterpriseRoot

Once a name is determined fitting to organizations naming conventions, "Next" is clicked. Following that, administrators will be asked to provide a location for both the certificate database and the certificate database log. It is recommended that these be stored in locations other than the default locations, and preferably on a different partition. While this is simply an attempt at "security through obscurity", it can be effective in thwarting casual attacks.

Following the placement of the various certificate components, it will be asked to stop ITS for the purpose of the installation, assuming this IIS server is not being used to host other websites, "Yes" is clicked. A query will be asked to enable Active Server Pages, which is necessary for the web enrollment service, here "Yes" is clicked again and then "Finish" is chosen from the Windows components Wizard.

4.4.2 Installing a Certificate on the Radius Server

From the server where RADIUS will be installed, Internet Explorer is used to browse to the certificate request page on the CA. For this wireless network, this will be <http://srv-2/certsrv>. It is fairly common for this site to be relocated for added security, if the CA was already in place

On entering, it will be prompted to enter a username and password, after successfully authenticating with the server, and then will be presented with the Microsoft Certificate Services website. Here the "Download a CA certificate is selected, certificate chain, or CRL" link from the "Select a task" menu. Next, the link that says "install this CA certificate chain" is clicked, which will allow the server to trust certificates issued from the CA server. The last step will be to click "Yes" to the dialog box informing that the website is adding a certificate to the computer.

Now that the CA's certificate is installed on the server, a computer certificate is requested for the RADIUS server itself. Since it is an Enterprise Certificate Authority, a

certificate using the "certificates" snap-in can be requested. To do this, the "Start" button is clicked, followed by clicking "Run ..." and then typing *mmc* and then clicking "Ok". From the File menu inside Console1, the "Add/Remove Snap-in" is chosen.

Next, the "Add..." button is selected from the bottom of the "Add/Remove Snap-in" window, and "Certificates" is chosen followed by clicking "Add". After that, "Computer Account" is selected to manage the type of certificate and then "Next", and "Finish". The "Close" on the "Add Standalone Snap-in" window is selected and then "Ok" is clicked in the "Add/Remove Snap-in" window.

Once back inside the Console1 window, the "Certificates (Local Computer)" is expanded and then right mouse clicked on "Personal", and from "All Tasks", "Request New Certificate" was chosen. This will spawn the "Certificate Request Wizard", from here "Next" is clicked. Then from the "Certificate types" field, "Computer" was chosen and then "Next" was clicked. A name for the certificate was entered, such as the server name, and then "Next" was clicked. Finally, on clicking "Finish", it will notify that the certificate request was successful; so "Ok" was selected. Now, a computer is made with certificate installed that can be used for the PEAP authentication of the wireless users.

4.5 INSTALLING AND CONFIGURING A RADIUS SERVER

Remote Authentication Dial-In User Service (RADIUS) is an industry standard protocol used to provide authentication. A RADIUS client (typically a dial-up server, VPN server, or wireless access point) sends user credentials and connection parameter information in the form of a RADIUS message to a RADIUS server. The RADIUS server authenticates the RADIUS client request, and sends back a RADIUS message response. There are a number of RADIUS products available on the market today, such as Funk Software's Steal Belted RADIUS; however Microsoft's implementation is just fine. Installing a RADIUS server using Microsoft Internet Authentication Service is extremely

straight forward and the management of it is just as easy, and most importantly, it comes free with Windows 2000 and 2003 server products [28].

4.5.1 IAS Installation

To begin the installation, the control panel is opened on the server where RADIUS would be implemented, and the "Add /Remove Programs" applet was opened. From there, the "Add /Remove Windows Components" button was clicked. A Windows Components Wizard will appear afterwards; the "Networking Services" option will be selected by scrolling down and then it will be double clicked. Next, a check in the box next to "Internet Authentication Service" will be placed and then "OK", "Next", and "Finish" options will be selected. Internet Authentication Service (IAS) is now installed and ready to be configured.

4.5.2 IAS Configuration

Configuration of IAS is done through the Internet Authentication Service console and can be found by clicking "Start", "Run", and then typing `ias.msc` and hitting enter.

Once inside the console, the first thing that needs to be done is registering the IAS server with Active Directory. This is done by simply right mouse clicking on "Internet Authentication Service (Local)" at the top of the left hand pane and clicking "Register Server in Active Directory". After that, a pop up will appear asking if the computer is authorized to read the users' dial-in properties (necessary to authenticate users in Active Directory). The okay option will be selected, and then the message confirming that the computer is now authorized will also be responded.

Next RADIUS clients need to be established. These clients are computers that are allowed to make requests of the RADIUS server, and then the server replies with a "Yes or No" type of answer to the client based on the settings in Active Directory. In this case, the

ISA server and the wireless access points will both be clients of the RADIUS server as both will be making requests to the server. The ISA will be requesting access for the purpose of authenticating VPN access and the access points will be requesting information for the purpose of WPA authentication. To create these clients, the "RADIUS Clients" will be right mouse clicked in the left hand pane of the console window and "New RADIUS Client" chosen.

Inside the "New RADIUS Client" dialog box, a "Friendly name" and the "Client Address" is entered. The "Friendly Name" is simply a name that is easy for the administrator to remember. For the ISA server, it is simply named as "ISA Server" and then the IP address of the internal interface card of that server will be entered, followed by clicking "Next" as shown in figure 4.7.

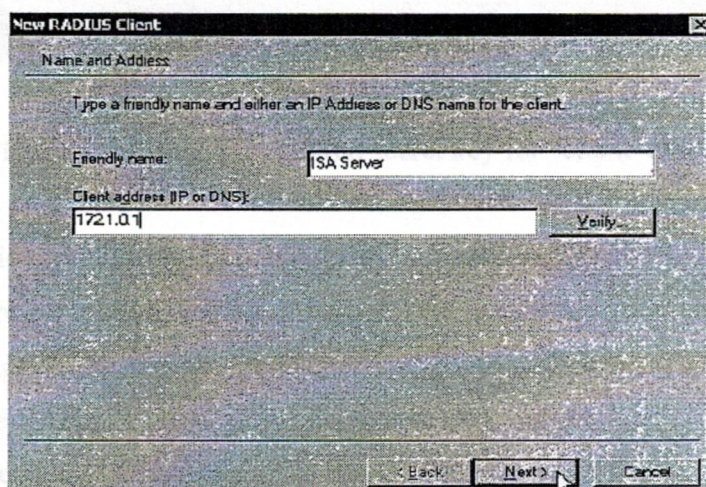


Figure 4.7 creating a name and putting in an IP address

Next, the "Client-Vendor" is to be specified which for both the clients will be "RADIUS Standard", and a "Shared secret" is entered. The shared secret for the ISA server will be *pen is mightier*. When planning for the shared secret, it is important to make it complex as possible, Microsoft recommends a minimum of 22-characters with a "random sequence of letters, numbers, and punctuation" to protect against dictionary type of attacks.

Additionally, a check is put in the box next to "Request must contain message authentication attribute".

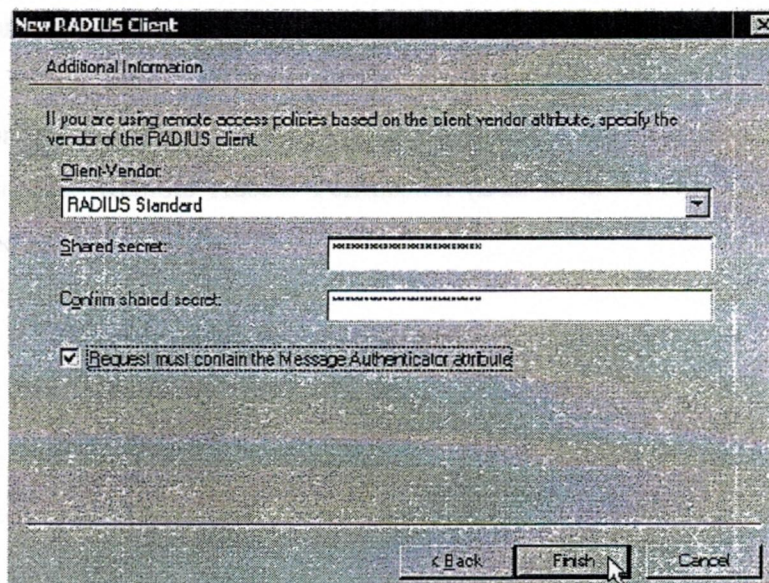


Figure 4.8 entering the shared secret key for "client-vendor"

To provide protection from spoofed Access-Request messages and RADIUS message tampering, each RADIUS message can be additionally protected with the RADIUS Message Authenticator attribute, which is described in RFC 2869, "RADIUS Extensions." The RADIUS Message Authenticator attribute is a Message Digest 5 (MD5) hash of the entire RADIUS message. The shared secret is used as the key. If the RADIUS Message Authenticator attribute is present, it is verified. If it fails verification, the RADIUS message is discarded. If the client settings require the Message Authenticator attribute and it is not present, the RADIUS message is discarded.

After those configurations are set, the client configuration is finished by clicking "Finish". This process will then need to be repeated for each of the RADIUS clients.

4.6 CONFIGURING AD USERS AND THE RADIUS POLICIES FOR ACCESS

There are actually two ways to allow users to authenticate through a RADIUS server; one through Active Directory, and the second through the remote access policy on the RADIUS server itself. In this network, the first option is selected as it's easier to configure. For this purpose, each user's property sheet needs to be configured in Active Directory, and the "Remote Access Permission (Dial-in or VPN)" attribute to "Allow access" will be set (Figure 4.9).

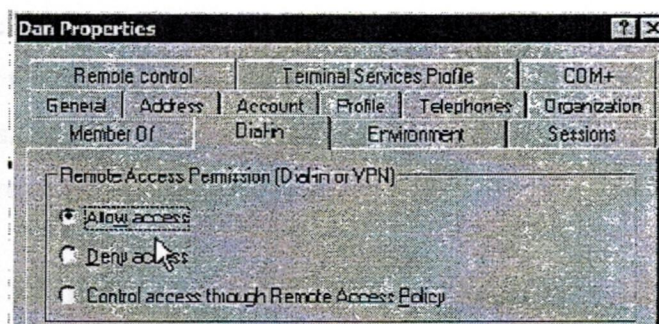


Figure 4.9 configuring remote access of AD users in Radius server

4.7 MICROSOFT INTERNET SECURITY AND ACCELERATION SERVER 2004

Microsoft Internet Security and Acceleration (ISA) Server 2004 is the advanced packet and application-layer inspection firewall, virtual private network (VPN), and Web cache solution that enables enterprise customers to easily maximize existing information technology (IT) investments by improving network security and performance. ISA Server contains a full featured, application-layer aware firewall that helps protect organizations of all sizes from attack by both external and internal threats. ISA Server performs deep inspection of Internet protocols such as Hypertext Transfer Protocol (HTTP), which enables it to detect many threats that traditional firewalls cannot detect. The integrated firewall and VPN architecture of ISA Server supports filtering and inspection of all VPN

traffic. The firewall also provides VPN client inspection for Microsoft Windows Server 2003-based quarantine solutions, helping to protect networks from attacks that enter through a VPN connection. In addition, a completely new user interface, wizards, templates, and a host of management tools help administrators avoid common security configuration errors.

4.7.1 Installing and Configuring Microsoft ISA Server 2004

As with any type of installation, it is important to harden the operating system itself against attacks before configuring services to run on it, and then check configurations at the end to ensure that the best practice has been followed on recommendations for those particular services. Since this server will be a frontline of defense for the network while configured as a firewall, this is especially true.

Since, the RADIUS server mentioned in the network is a member of network's domain; all wireless users will be authenticated using their domain user account credentials, regardless of the membership of the ISA server itself. That being said, either configuration; an ISA server as a member of a workgroup or of a DMZ domain, will function the same as it pertains to the configuration in this chapter.

First, the ISA server needs to have its network adapter cards configured with the appropriate addresses. All interfaces should be configured with static addresses, with the exception of the interface that is attached directly to the internet, which can use a DHCP assigned address. Since extra configuration is required of the ISA server to accept and use a DHCP assigned address, this configuration type will be used during the installation and configuration segment. It is also recommended to assign a recognizable name to each interface to make setup and administration of the ISA server easier.

Once the operating system is sufficiently locked down and the IP addresses configured, the installation and configuration of Microsoft ISA Server 2004 can be started.

The installation of Microsoft ISA Server 2004 (ISA) is fairly straight forward [29]. Inserting the program CD and selecting Install ISA Server 2004.

The installer is prompted to accept the normal Microsoft agreement and then prompted for User Name, Organization, and Product Serial Number. The values that are required must be entered and the process is continued by choosing "Next". At the next screen, "Typical" is chosen and then "Next". The following screen requests that the installer specify the internal address ranges.

Add is selected and then the "Select Network Adapter" button is clicked. On the screen that follows, the box that says "Add the following private ranges..." is unchecked and then the box that is next to the adapter card of the internal network is checked, followed by clicking the "OK" button (Figure 4.10).

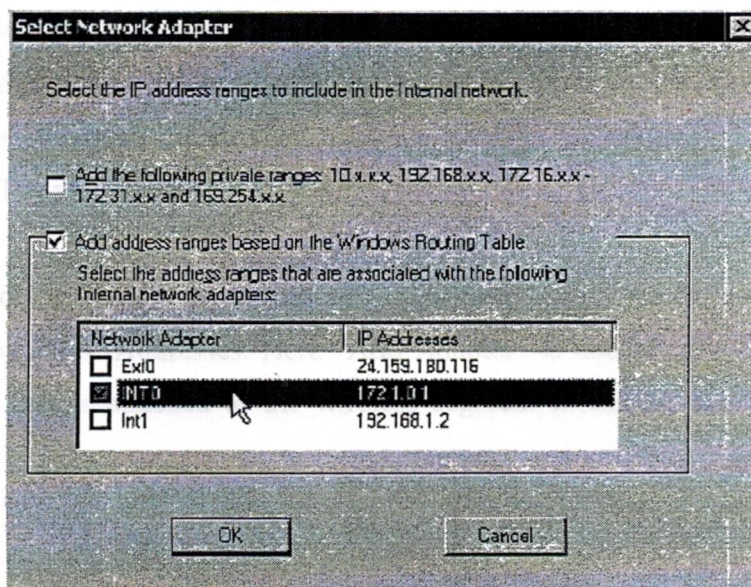


Figure 4.10 choosing appropriate IP ranges

The installer will be presented with a warning about miss configured routing tables, "OK" was selected, and "OK" and then "Next" were clicked. Selecting "Next" to the

remaining prompts and ISA will install. Once the Installation Wizard Completed screen appears, a check is placed in the box next to "Invoke ISA Server Management when the wizard closes" and "Finish" was selected. At this point the Microsoft Internet Security and Acceleration Server 2004 management console will appear, here, the "Firewall Policy" link is clicked in the left hand pane and the firewall policy list in the right hand pane. By default ISA installs with the "Last Default rule" which blocks all access to all networks and serves as a catch all to deny access to anything that has not been explicitly allowed by the administrator.

To simplify the configuration process of ISA Server, Microsoft has provided with various configuration templates that serve as great starting points for the configurations. At this point, the "3-Leg Perimeter" template is selected. If there is already an ISA firewall configuration in place, applying these templates will delete current running configuration. It is recommended, to try these configurations out on a non-production server first and then add the policies that are needed to run the configuration. From the ISA management console, "Networks" under "Configuration" on the left hand pane was selected, and then the "Templates" tab from the far right pane was clicked. On clicking "3-Leg Perimeter", the "Network Template Wizard" will begin.

On clicking "Next" a portion of the wizard comes which asks to define the Perimeter Network IP Addresses. Here "Add Adapter" is clicked, and then the network interface card that is attached to the wireless segment is chosen and "OK" is clicked (Figure 4.11)

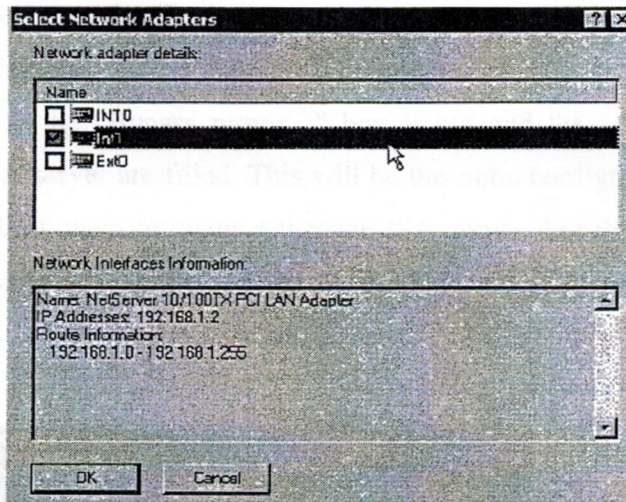


Figure 4.11 selecting network adapters.

After selecting "Next", the selection of a firewall policy is done by choosing "Block All", then "Next", and then "Finish". Then the template installation is finished by clicking "Apply" from the top of the screen.

After the initial installation is complete, it is recommended to download any updates to ISA 2004 that may be available. As of this writing, ISA Server 2004 Service Pack 1 is the latest patch for the application.

4.7.2 Checking For Internet Connectivity

Generally, if a client wants to connect to the internet through the ISA server, or any other network for that matter, a rule must be created to do so. However, as part of the default System Policy on the ISA server, the local system (the ISA server itself) can connect to *.microsoft.com, *.windows.com, and *.windowsupdate.com with no rule changes / additions to the Firewall Policy [30]. In order to connect to those web sites though, one change needs to be made to browser so that it will connect to the internet using ISA. To configure this setting in Microsoft Internet Explorer (IE), IE is opened and the "Tools" link is clicked on the main menu bar and then "Internet Options". From here, the

"Connections" tab and then the "LAN Settings ..." buttons are selected from the bottom. In the "Local Area Network (LAN) Settings" dialog box, a check in the "Use a proxy server..." box and in the "Bypass proxy ..." box is put and the address of the internal interface card on ISA server are filled. This will be the same configuration used on all the internal clients to allow them to connect through ISA server. For the test network in this chapter, this address is 172.1.0.1 followed by the standard ISA port of 8080 shown in figure 4.12.

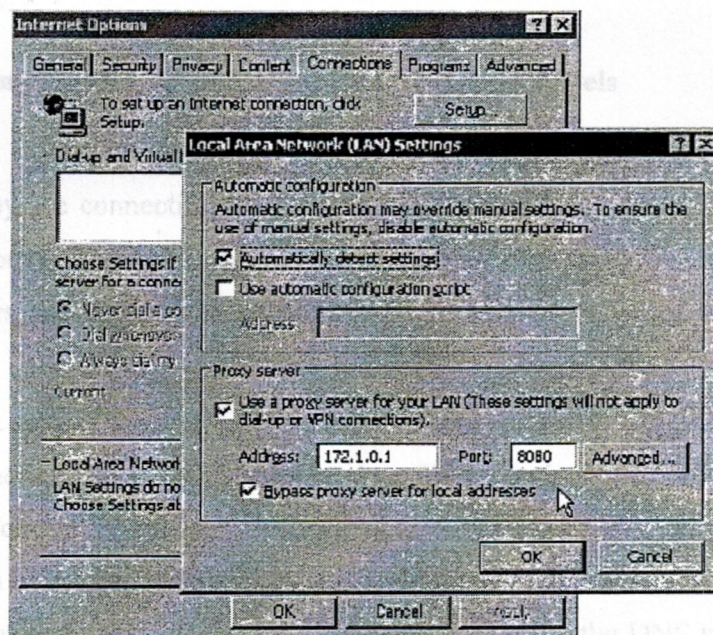


Figure 4.12 configuring the LAN in IE

Following entering the appropriate numbers, "OK" and "OK" are clicked, IE is closed and then reopened again. At this point it will be able to browse to www.microsoft.com and confirm the configuration.

If at any point the ISA server stops providing a service that it is configured for, consulting the "Dashboard" is an excellent place to start the troubleshooting efforts. The

"Dashboard" is located in the ISA management console by clicking the "Monitoring" link on the left hand pane, and then selecting the "Dashboard" tab from the right hand pane.

The "Alerts" section of the "Dashboard" will notify the administrator of any misconfigured rule, critical system and server information, and all other alerts configured for the server. This function is surprisingly valuable, and does an excellent job at pointing out problem areas in the server and giving advice as to how to fix the problem. As an ISA administrator, this "Dashboard" area is something to become very familiar with.

4.7.3 Configuring the ISA Rules for the Desired Access Levels

Charting out what protocols and hosts should be accessible to VPN clients, especially if they are connecting from the internet side of the firewall, deserves a lot of planning and thought. For those administrators, who wish to simply grant internet access to the wireless users, this step will be quite simple, but for some, it will never be sufficient.

The first policy that will be explored is one that will allow the internal DNS forwarder to function properly, and ultimately will be required for wireless clients to surf the internet, which will be the next rule to look at. A forwarder is a Domain Name System (DNS) server on a network used to forward DNS queries for external DNS names to DNS servers outside of that network. To use forwarders to manage the DNS traffic between the network and the Internet, the firewall used by the network is configured to allow only one DNS server to communicate with the Internet. When the other DNS servers in the network are configured to forward queries they cannot resolve locally to that DNS server it will act as a forwarder. This is accomplished by right mouse clicking the "Firewall Policy" link, and selecting "New" and then "Access Rule".

To begin with the first rule, right mouse is clicked on the "Firewall Policy" link on the left hand side and then "New" and "Access Rule" are chosen. The next step in the process will require a bit of decision making. It is easier to create rules for computers / networks and then configure the rules for the protocols desired for those computers /

networks. This first rule will be for a DNS forwarder, which in the case of network, the DNS server is named SRV-2, and the traffic will be flowing from the server to the internet. With this in mind, the rule will be named *SRV-2 > Internet*. Using this line of thought, any other protocol SRV-2 is allowed to send to the internet can be added to this rule later.

Once a naming convention is established, and the name for the rule is entered, "Next" is clicked. The next screen determines the rule action. In this case, a rule is created to allow for access, so "Allow" is selected, and then "next" [31]. Following this, an appropriate protocol for the rule is selected. To do this, the drop down menu is used and "Selected protocols" is selected and "Add..." from the right.

The protocols are all organized in easy to recognize folders by their function and some are overlapping. DNS, for example, is an "Infrastructure" protocol, but can be found in the "Common Protocols", (Figure 4.24) "Infrastructure", and "All Protocols" containers. To select DNS, the "Infrastructure" container can be expanded where "DNS" is selected and "Add" is chosen as in figure 4.25.

Since SRV-2 will not be hosting DNS records for internet users to query, it is not necessary to add "DNS Server". There are several other protocols available in which there are both an application protocol and an application server protocol.

After the DNS protocol has been added, to close the "Add Protocol" window "close" is chosen, and then "Next". The next screen will ask who the traffic for this rule will come from, to add SRV-2, "Add" will be clicked and "New" and "Computer" will be selected and appropriate information will be filled and Okayed as shown in figure 4.26.

This process will then add that server to the toolbox, and it can be used again as needed. This process will eventually need to be repeated for each computer / network that will have a rule made involving it.

After clicking "OK", the "Computers" container can be expanded and the SRV-2 object just created will be double clicked, and then "Next" from the "Access Rule Sources" page will be selected. Now, it should be defined where the traffic is going, which is done with the same process as before, by clicking "Add", and this time just expanding the "Networks" container and double clicking "External", "Close", and then "Next". The next screen allows restricting the users who are authorized to use this rule from the client machine. For the purpose of this rule, the "All Users" group is fine, so "Next", "Finish", and then "Apply" are selected simultaneously. Now the internal DNS server will be able to forward DNS requests to the internet.

A rule will also need to be created allowing the wireless access points to send their RADIUS traffic to the RADIUS server itself. To do this, a rule is created for RADIUS and RADIUS accounting, and instead of adding each wireless access point individually, they can be added as a group. Instead of choosing "Computer" from the "New Rule Element" drop down menu, the "Computer Set" option is chosen, named, and then all the wireless access points are added to it.

The previous rules allowed access to a computer or network for the purpose of using a specific protocol. The next set of rules, are rules that allow the firewall to act as a proxy for that service, making it appear that the firewall is the one actually hosting the service. This function will be utilized to publish an internal DNS server to the wireless perimeter so that the VPN clients can resolve the name of the VPN server they are attaching to. This will allow simplifying the client configuration and allowing that client to connect regardless of which arm of the network they are attaching from. This type of rule is also the type of rule used to publish a web server or mail server. To create this rule, the right mouse is clicked again on the "Firewall Policy" link on the left from where "New" and then "Server Publishing Rule" are chosen. It should be noted that for publishing rules, only one protocol can be published per rule. Following adding the name, "Next" is clicked. The next screen requests the server IP address, and in the case of this network, it is 172.1.0.2, configure that and then "Next". The protocol are selected from the drop down

menu, and as mentioned previously, it is a publishing service, so DNS Server should be chosen (conveniently Microsoft limited the choices on this drop down box to the services objects), and then "Next". Since, it's just for publishing the service to wireless users; the "Perimeter" network from the list of networks is selected to listen on, and then "Next", "Finish", and "Apply" are clicked.

4.8 CONFIGURING THE WIRELESS ACCESS POINTS

Configuring access points is similar between the different models and manufacturers, however it is important to remember, that access points other than those outlined here will most definitely be different.

In order to configure the setup, it should be kept in mind that different revisions of the firmware installed on the access points may differ in their configuration and available options; it is recommended to consult with the manufacturer for the latest available firmware updates.

Additionally, if buying new hardware is in consideration, its best to consult the manufacturers' website to determine the AP that is right for the network that it is going to get deployed into. Without question, the access points should support WPA if not the full 802.11i standard, which as of this writing will provide the best level of security currently available.

4.8.1 Configuring a Linksys Access Point

The following is the access point (Table 4.4) used in this section of the chapter [32].

Table 4.4 a Linksys Access Point

TWAPI	
Manufacturer	Link Sys
Model Number	WRT54G ver.2
Firmware Version	V3.03.06
IP address	192.168.1.11

Before beginning the configuration portion of the install, it is important to point out that doing the initial install of the access point is easier done attached to a workstation instead of the ISA server. This will help rule out any problems encountered as being firewall rule related and will minimize random rule creation such is common during moments of frustration with an ISA server.

Once the initial configuration is set, the access point is plugged in to the network interface card designated on the ISA server for the wireless perimeter network and ensured that the end attached to the access point is plugged into a LAN port and not the WAN port. This particular model of access point can also function as a broadband router, which is what the WAN port is intended to service, however for the purpose of this installation, this functionality will not be needed.

It could be argued that the WAN port be utilized as means of adding extra protection for the wireless network, however it is always recommended that the level of protection offered by this solution is minimal compared to the amount of extra configuration required to gain it. The use of a wireless router instead of just an access point is indicative of networks that have hardware currently in place that is being redeployed to meet the configuration scenario represented here. To begin the configuration process, the setup procedures for the initial install are taken into consideration. Once the initial setup is complete, one can log into the access point and click on the "Administration" tab. Here the router password is changed to a secure password which can be a maximum 32 characters,

but unfortunately cannot include any spaces. Also, the web access is changed from HTTP to HTTPS by un-checking the box next to HTTP and putting a check in the box next to HTTPS, and disabling Wireless Access Web by selecting the "Disable" radio button. A layout of a typical Linksys router is shown in figure 4.13.

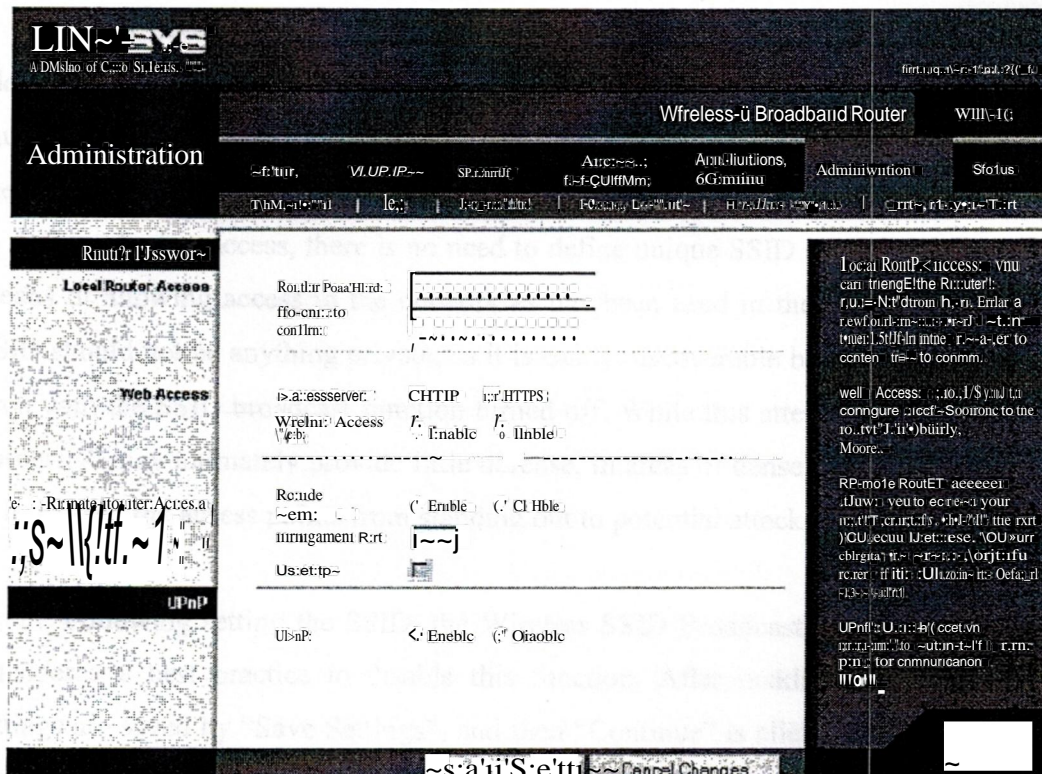


Figure 4.13 Linksys Administration Panel

This will ensure the use of a strong password over an SSL connection and will also keep the wireless users from being able to manage the access point. Selecting "Save Settings" will commit the changes and then the certificate for the access point will be added when prompted on login. Now, the session is secured using SSL and any further communications will be protected.

Next, the "Wireless" tab is selected and "Basic Wireless Settings" link is clicked. First the Wireless Network Mode is chosen from the list of Mixed Mode, B-only, or G-

only. For the wireless network, the only clients that will be connecting are G compatible, so G-only will be selected. In mixed mode, both B and G mode clients will be able to connect, but the connection speed will be slowed to the lowest common denominator. If there are 10 G clients and 1 B client, all 11 will communicate at B speeds.

After deciding the network mode, the wireless network is assigned a service set identifier (SSID) name. This SSID is nothing more than, as the name implies, an identifier, much the same way that workgroup names define workgroups. For most networks, using the same SSID throughout the organization is acceptable, and since RADIUS will be used to define who has access, there is no need to define unique SSID and encryption keys as a means of allowing access to the network as has been used in the past. Additionally, this SSID should not be anything private, as it is easily discoverable by wireless sniffing tools, even with the SSID broadcast function turned off. While this attempt at "security through obscurity" may ultimately provide little defense, in areas of dense wireless activity, it may at least keep the access points from standing out to potential attackers.

Following setting the SSID, the Wireless SSID Broadcast is "Disabled". It is still considered a best practice to disable this function. After making these selections, the settings are saved by "Save Settings", and then "Continue" is clicked from the screen that pops up.

The next step is to define the wireless security mode. So, the "Wireless Security" link is selected and then using the drop down menu "WPA RADIUS" is selected.

Selecting WPA RADIUS will then allow for entering in the appropriate RADIUS server information. The first option is which WPA Algorithm to use; TKIP 'Temporal Key Integrity protocol', or AES, 'Advanced Encryption Standard'. While TKIP is not actually an algorithm, it is a key management protocol; the important thing to note is that AES is part of the new WPA2 standard, and is not backward compatible to devices that only support WPA.

It is important to take into account all of the access points on the network, and what they support, as this will determine whether to use AES or TKIP. By configuring all the access points identically, users who have access rights through RADIUS to roam will be able to move about between these access points with relative seamless connection; while reducing the administrative burden of configuring the clients and access points. While the XP client that comes with Service Pack 2 supports AES, one of the access points used on the network does not, so all access points on the network will be configured for TKIP. If all of the access points and clients will support AES, AES might as well have been chosen here and in the client configuration as well.

Next, the appropriate information is entered into the remaining fields. As per the configuration of the network, the RADIUS server address is 172.1.0.4, the RADIUS port is the default 1812, the Shared Key is *pen is mightier*, and the Key Renewal Timeout can be left at the default value of 3600.

Following these changes, settings are saved by clicking on "Save Settings" and then "Continue" from the next screen. Additionally, since this particular unit is a router and also a gateway, a route should be added to its routing table so that it knows where 172.1.0.4 actually is. To do this, the "Setup" link is clicked followed by the "Advanced Routing" link. For the operating mode, "Router" is chosen from the drop down menu, and then "LAN & Wireless" from the RIP drop down menu.

Then, a name needs to be assigned for the route, such as "TWAPtoInternal" (the name cannot contain spaces), and then the appropriate IP information is entered. For this network domain, the destination LAN IP is 172.1.0.0 and the subnet mask is 255.255.0.0, and the default gateway is 192.168.1.1, which is the perimeter facing interface card of the ISA server.

These settings are confirmed by clicking the "Save Settings" button, followed by clicking the "Continue" button.

Finally, this unit needs to be set up to handle DHCP requests for the wireless users. This is done on the "Setup" tab and under "Basic Setup". The DHCP is enabled by selecting the radio button across from "DHCP Server", and then the starting address are entered followed by the number of clients who will be connecting. For the network, those values will be 192.168.1.100 and 50 respectively. Also, the DNS server is configured to the address 192.168.1.1, as this is the address of the perimeter facing network interface card of the ISA server that is now publishing the DNS service to the network. The configuration is saved by clicking "Save Settings" and then "Continue".

For the purpose of this network, this is all that needs to be configured on the access point; however, for additional security into the network, Wireless MAC Filter protocol should definitely be employed. The way the MAC address filtering works is simply allowing or disallowing access based upon the wireless interface card's Media Access Control (MAC) address, which is an address assigned to the card from the manufacturer. However, creating these MAC address lists can be quite laborious for a large number of clients, which will need to be repeated for each access point. This option simply doesn't scale very well. Additionally, MAC addresses can be spoofed by attackers; meaning a malicious user can monitor the wireless traffic and collect a list of MAC addresses that are able to communicate on the network, and then mask the MAC address of their interface card with one that is permitted on the network, thus bypassing this security measure. But this measure can still be used which makes another layer of security in the wireless network.

4.8.2 Configuring a D-Link Access Point

For the explanation, this specific D-Link access point was employed [33]. The specs are shown in table 4.5.

Table 4.5 D-Link access point

TWAPI	
Manufacturer	D-Link
Model Number	DI-624 Revision C3
Firmware Version	2.50
IP address	192.168.1.12

The configuration process for the O-Link is much the same as the Linksys. Again, the model used is a wireless router instead of just an access point, so there is lots of functionality that will not be utilized. Most of the interfaces look the same across vendor platforms; however, as mentioned before, the routers will have additional links to the extra functionalities, which can be utilized accordingly.

On the configuration side, the D-Link unit actually has a convenient wizard that takes administrators through the basic setup process, including changing the admin password.

After this initial setup and with the "Home" tab selected, the "Wireless" link on the left is clicked to open the properties sheet for the wireless settings. This is the page where the wireless security settings can be configured. The page layout is shown in figure 4.14.

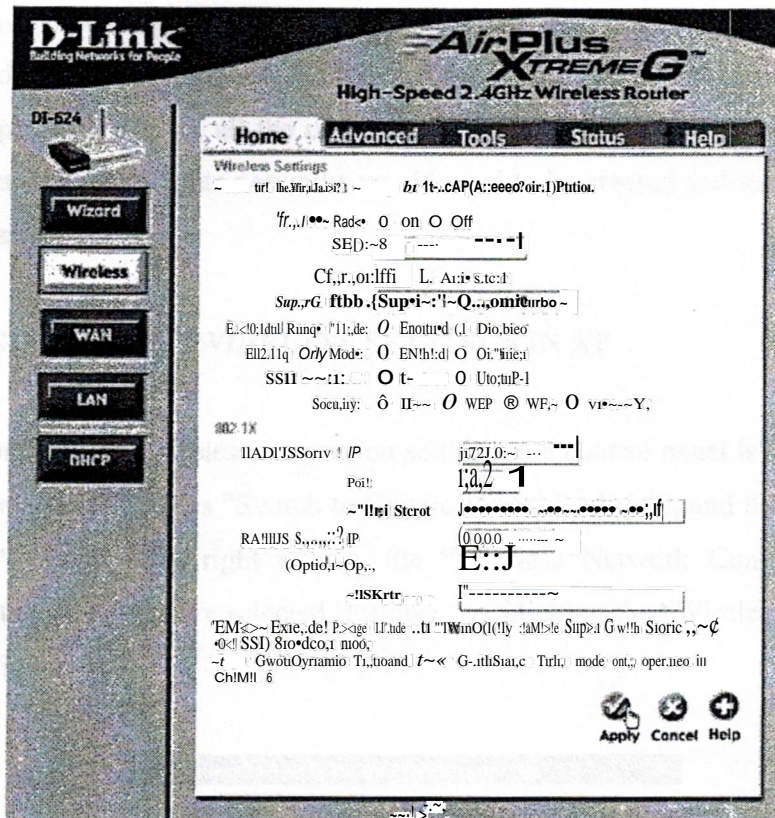


Figure 4.14 security settings in D-Link access point

While the interface looks different from the Linksys model, all the basic configurations are the same, with a few exceptions. First, it is noticed that there are extra modes that this unit supports such as Super G mode and Extended Range Mode. These additions are proprietary options and do not work unless a D-Link wireless interface card is used that is suited for those modes. These types of "extra frills" are common among the different wireless vendors; however they usually are not compatible from vendor to vendor. Secondly, this particular unit does not have an option to choose between AES and TKIP as was available with the Linksys. After conducting a brief experiment with the client, by trying to connect to the access point using AES and then TKIP, it was determined that this model only supports TKIP.

Because this particular unit only supports TKIP, all the access points in the network will also need to be configured to use TKIP. Likewise, had this access point only supported WPA-PSK (pre shared key), all the other access points would need to be configured for WPA-PSK as well, or separate networks would need to be created and roaming would not be as seamless.

4.9 CONFIGURING THE WIRELESS SETTINGS IN XP

To configure the wireless connection settings, the control panel is accessed and the link in the upper left that says "Switch to Classic View" is clicked, and then the "Network Connections". Next, using right mouse, the "Wireless Network Connection" icon is selected and the properties are selected, followed by clicking the "Wireless Networks" tab as shown in figure 4.15.

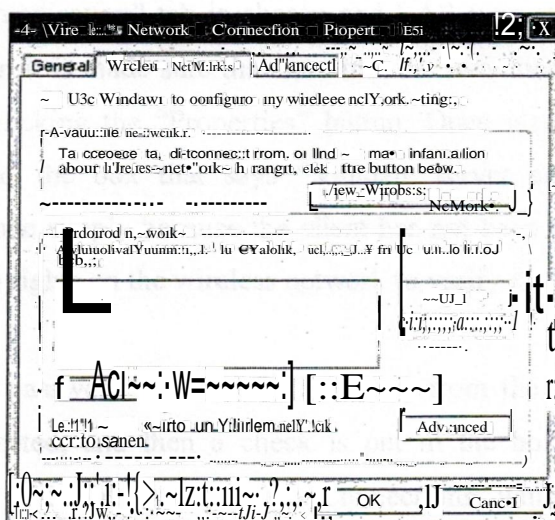


Figure 4.15 Wireless network configuration panel of XP

From inside the "Wireless Network Connection Properties" window, the "Add" button is clicked. On the association tab, the SSID is entered which is the same as entered on the access points, and then the "Network Authentication" is changed to "WPA" and the "Data Encryption" to "TKIP" shown in figure 4.16.

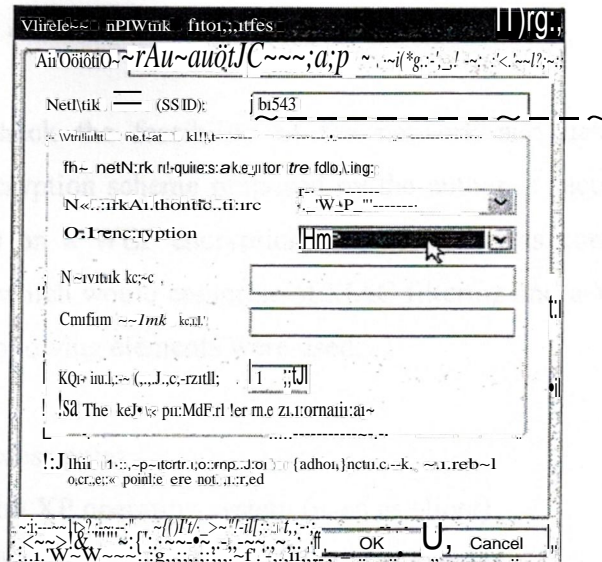


Figure 4.16 choosing SSID and encryption type

Next, the "Authentication" tab is chosen and EAP type is changed to "Protected EAP (PEAP)", and then it is made sure that the two check boxes below that are cleared, followed by clicking the "Properties" button. Once inside the "Protected EAP Properties" dialog box, the box that says "Validate server certificate" needs to be unchecked, which is done simply because the client has not been given a certificate from the root CA, and has no rights on the wireless network to verify it.

Next, "Secured password" (EAP-MSCHAP v2) from the authentication methods drop down box is selected, and then a check is put in the box next to "Enable Fast Reconnect", then click "OK" until the "Network Connections" window.

Once this is finished, the wireless network should automatically connect, using the Windows domain user credentials for authentication. If it does not connect automatically, the option "Wireless Network Connection" is selected and "View Available Wireless Networks" is chosen. Here, the wireless network configured from the previous step is selected and then "Connect" from the lower right hand corner.

4.10 COMPARISON AND CONCLUSION

In order to check the feasibility of the network and determine whether the authentication and encryption scheme proposed by the author is secure as compared to a network which works on a WEP encryption, the network was compared with another network environment which would comprise of MAC filtering and a WEP encryption. For testing purposes, the following elements were used:

- 1- AD-Link access point
- 2- A Laptop with XP operating system (used as client)
- 3- A desktop computer with a WLAN PCI card installed
- 4- Netstumbler 0.4.0 (Build 554)
- 5- Airodump ver 3
- 6- Aircrack ver 2.3

The O-Link access point was configured with the following configurations:

- 1- ESSID = aikldo2three3a
- 2- MAC filtering
- 3- DHCP broadcast
- 4- WEP encryption = bre0ak6me3if8u9can

Because WEP can work on an alphanumeric pattern, digits as well as alphabets can be taken into consideration.

The same configuration was taken in account for the network proposed by the author, the only difference was installing some more authentication mechanisms which were proposed earlier, like using a Certificate Authority for authenticating the access point as well as the client, plus using TKIP instead of a WEP protocol, but the encryption key was kept the same as described in the scenario above.

So, first the network was tested using just a WEP encryption, using the D-Link access point as the medium of connection between the laptop and the server. A desktop computer was used a biquad antenna in another room for collecting enough packets traveling in the air between the access point and the client laptop. Netstumbler was used to analyze the packets sniffed through the air.

Netstumbler is an active MS-Windows based scanner that produces the information necessary for mapping Wi-Fi hotspots including ESSID, encryption and GPS co-ordinates. Since the program constantly sniffs for active packets in the open, the responses are more abundant. NetStumbler is not self contained and it uses Windows drivers to access the WiFi card, causing the Wireless Zero Configuration to shut down when run. Wireless Zero Configuration in WinXP allows the operating system to find available WiFi networks. This is a problem for connecting to an access point while sniffing. The easiest way to resolve this is to save the NetStumbler data, close the program, and refresh the available networks. A screen shot of Netstumbler is shown in figure 4.17.

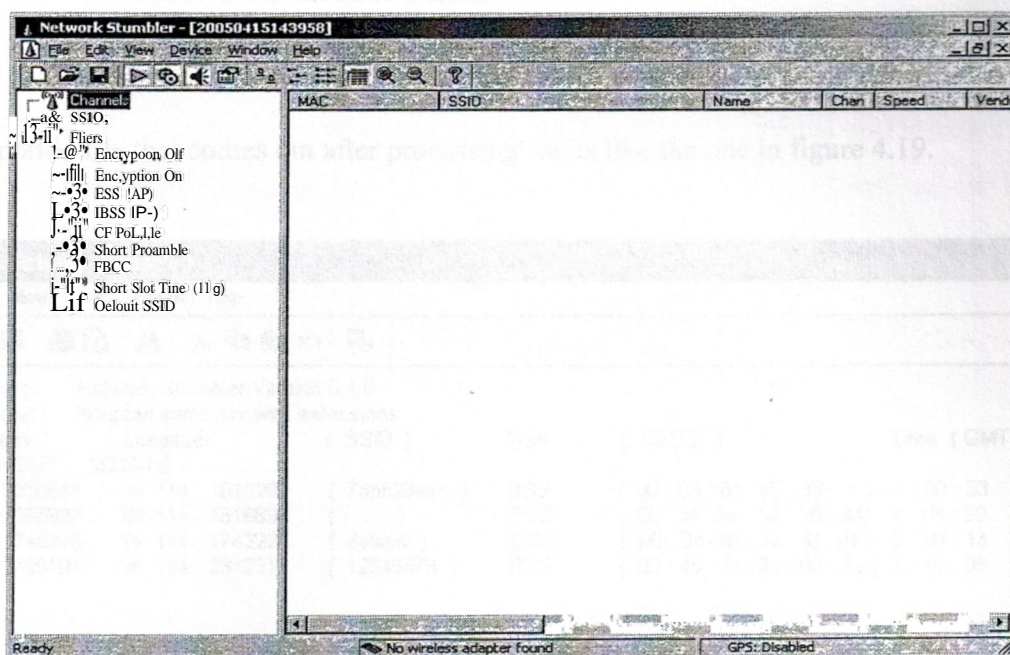


Figure 4.17 a Screenshot of Netstumbler

After setting up everything, the antenna was focused in the direction of the transmission and Netstumbler started sniffing the packets traveling in the air. The advantage of using the Netstumbler is the fact that it can use multiple formats for outputs, such as a CVS file or text. In this scenario, text format was selected as shown in the figure 4.18.

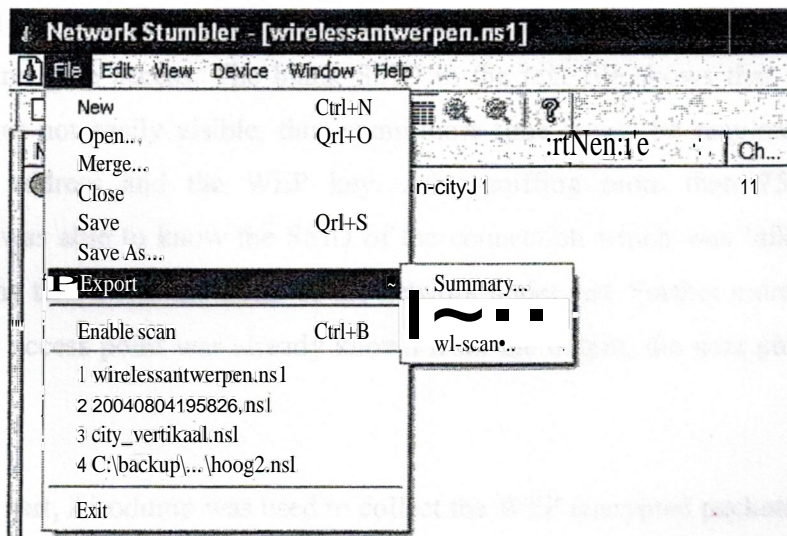


Figure 4.18 Selecting text as the medium of format

The exported file that comes out after processing looks like the one in figure 4.19.

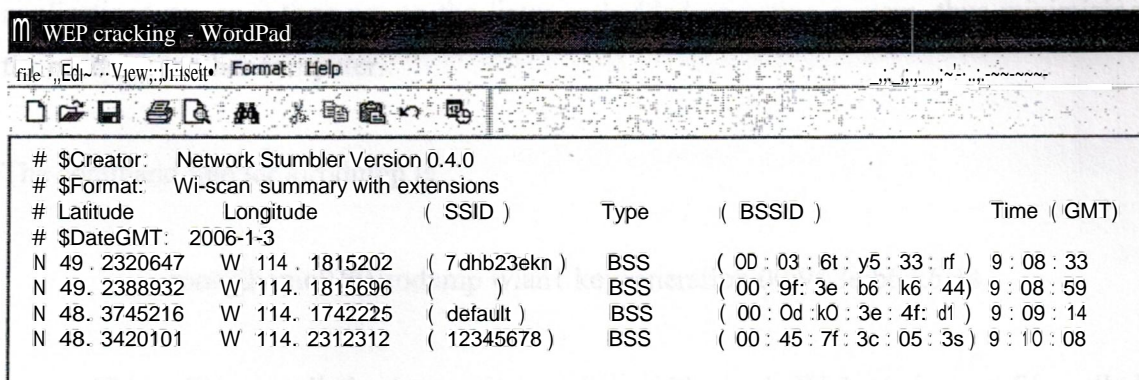


Figure 4.19 Netstumbler data exported into a text file

From the text file it can be seen that the networks which Netstumbler was able to sniff did not hide the SSID and this they were easily visible. And further more, if a laptop can have the same SSID and the access point is transmitting on a DHCP then, its quite easy to get an unauthorized access, because the laptop will have the same SSID and the access point will have no choice unless to give the laptop a new set of IP address. But, if the access point is not transmitting a DHCP address, or if the access point is using a MAC filtering, then the laptop will never be able to connect, as the access point will not authenticate and give access. The blank SSID in the text file shows that the SSID was hidden and was not easily visible, thus some more time would be required to know the SSID, MAC address and the WEP key. After sniffing more than 75,000 packets, Netwtumbler was able to know the SSID of the connection which was 'aikldo2three3a', thus confirming that it was the SSID of the network under test. Further more, as the MAC address of the access point was already known from the output, the next phase of the test was tried.

In this part, Airodump was used to collect the WEP encrypted packets, from which, the weak initialization vector packets were kept in a file called keygeneration and the unnecessary packets were dumped which would complicate the key generation process. Airodump works on a Linux operating system so, for this purpose, cygwin was installed on the desktop computer. Cygwin is a linux-like environment for windows, where the applications run as if they are on the linux embedded operating system, thus minimizing the need for another computer.

The command line for airodump is

```
-root@home[\\]#airodump wlanl keygeneration 00:9f:3e:b6:k6:44
```

This will save all the interesting packets with weak IV keys in one file called keygeneration.txt which could be then analyzed in Aircrack.

Figure 4.20 Netstumbler data captured into another text file

Aircrack is an 802.11a/b/g WEP/WPA cracking program that can recover a 40-bit, 104-bit, 128-bit, 256-bit or 512-bit WEP key once enough encrypted packets have been gathered. So, the Aircrack utilizes the keygeneration.txt file developed by the Airodump and start the cracking process to generate the correct key. To break a 128-bit WEP key, the text file will need to have almost 300,000 to 800,000 of unique IV packets. Sometimes, it will take more than 15 hours to collect this much data, depending upon the strength of the WEP key. Using Aircrack, the command will be

```
- root@home[~]# aircrack-f2 -rn 00:9f:3e:b6:k6:44 -n 128 -q 3 keygen*.cap
```

If Aircrack finds the correct key, it says 'Key Found'. In this case, it was able to find the correct WEP key as

```
KEY FOUND! - bre*ak6me3if8u9can
```

It is noticed that there is a missing digit in the WEP key, which will be because the Aircrack was unable to distinguish that digit from 0 to o. But none the less, if more packets would have been captured, that possibility would also have been eliminated.

Then the test was repeated for the network with the enhanced authentication scheme with PEAP and TKIP in working state. Netwtumbler was again employed to sniff enough packets, so as to crack the TKIP key, but after collecting more than a million packets, the output of Netstumbler as the text file was as shown in figure 4.20.

f1 WEP cracking · Notepad									
File Edit Format View Help									
Network Stumbler version 0.4.0									
scan summary with extensions									
Longitude		C SSID)		Type	(aSSID)		I Time		C GMT)
ie-1-S									
W	114 . 1815202	C	7d9b23ekn)	ass	C	00 : 03 : 6t : y5 : 33 : rf)	18 : 09 : 21		
W	114 . 1815696	(a/'l.*o2l**n**))	ass	C	00 : xx : xx : xx : xx : xx)	18 : 22 : 22		
W	114 . 1742225	C	default)	ass	(00 : 0d : k0 : 3e : 4f : dl)	18 : 54 : 04		
W	114 . 2312312	C	12345678)	ass	(00 : 45 : 7f : 3c : 05 : 3s)	18 : 03 : 24		

Figure 4.20 Netstumbler data exported into another text file

From the data exported by Netstumbler, it was gathered that

SSID = al*|*021**n**

MAC= 00::XX::XX:XX:XX

Thus, it can be easily noticed that Netstumbler was not able to sniff what the SSID and the MAC address of the network was. The process was repeated for extended time period in which more than 10,000,000 packets were gathered for computation, and still, the result was almost the same.

4.11 SUMMARY

It is quite obvious that a solution needs to be presented to safeguard the wireless networks. Simply creating single layered defense for this problem has not worked in the past, and in fact, has fueled the distrust for wireless implementations. However, by combining the strength of the RADIUS server and 802.1x standards with ISA server and PEAP authentication, a stronger and secure network was implemented and then tried and tested to check the feasibility of the network, thus giving appropriate and encouraging results.

It was observed after an extensive testing that the network which depended on the WEP encryption is quite vulnerable and the WEP attacking tools exploit the vulnerabilities in the WEP key to expose the useful encrypted information, such as the SSID, MAC address and the WEP itself to an unauthorized user.

5. CONCLUSION

Wireless Local Area Networks have been in deployment since years now, but their level of security is still a matter of concern to both the clients and administrators. And new advancements in software designs and wireless packet sniffing tools have made the scenario worse. It's not a matter of hours, or even minutes until the wireless network is compromised and security breached.

The wireless communication world is thriving to invent new and more powerful security protocols, like Kerberos, EAP, TLS, AES and many more to make a wireless local area network as secure as possible. New ways are invented to tackle the sniffing tools and various attacks done by an anonymous object or entity outside the network.

Taking into account the security issues, a wireless network is developed that has enhanced authentication and difficult to get compromised. For authentication purposes, a Certificate Authority (CA) Server was placed in the Protected Extensible Authentication Protocol (PEAP) authentication mechanism, which comprises of Remote Authentication Dial-in User Service (RADIUS) Server, for delivering and checking the certificates and user credentials to and from the client, Domain Name Server (DNS) and Microsoft Internet Authentication and Acceleration (ISA 2004) Server for firewall and proxy purposes and managing the users in more robust atmosphere. The client equipment was also configured accordingly so that they could be automatically authenticated. Two prototypes of wireless access points were taken into consideration: A Linksys (WRT54G) Access Point and a D-Link (DI-624) Access Point.

It was showed after an extensive testing that the network which depended on the WEP encryption is quite vulnerable and the WEP attacking tools exploit the vulnerabilities in the WEP key to expose the useful encrypted information, such as the SSID, MAC address and the WEP itself to an unauthorized user.

6. REFERENCES

- [1] Ruber P. Wireless networks come of age. Retrieved on November 2005 from World Wide Web: <http://www.computeruser.com/articles/2104.1.2.1.0401.02.html>
- [2] Theodore, R.S. (December 2001). Wireless Communications: Principles and Practice. Prentice Hall, PTS.
- [3] Unger, J. (2003). Developing a License-Free Wireless Wide-Area Network. Indianapolis, Cisco Press.
- [4] Frater, Michael R., Rayan Michael J. (March 2002). Communications and Information systems. Argos Press Series.
- [5] Miller T., Monzingo R. (July 2004). Introduction to Adaptive Arrays. North Carolina, Scitech Publishing Inc.
- [6] Godarna L. (January 2004). Handbook of antennas in Wireless Communications. Boston, CRC Press LLC.
- [7] Higgins J. (February 2000). Satellite Newsgathering. Reed Educational and Professional Publishing Ltd.
- [8] Honcharenko, W., Kruys, J.P., Lee, D.Y., and Shah, N.J. (January 1997). Broadband Wireless Access, IEEE Communications Magazine, 20-26.
- [9] Atkinson R., and Kent, S. (November 1998). Security Architecture for the Internet Protocol. IETF, RFC 2401.

- [10] Arbaugh, William A., Narendar Shan.kar, and Y.C. Justin Wan. Your 802.11 Wireless Network has No Clothes. Retrieved March 18, 2005 from World Wide Web: <http://www.cs.umd.edu/~waa/wireless.pdf>
- [11] AirDefense, Inc. (October 05, 2004.) Best Practices for Rogue Wireless LAN Detection.
- [12] Rysavy, P. Wireless Broadband and other Fixed-wireless systems. Retrieved August 22, 2005 from World Wide Web: <http://www.networkcomputing.com/netdesign/bb1.html>
- [13] Lapres D.A., (1988). Multi-point Multi-channel Distribution systems. May.: 1-5.
- [14] Orthman F., Roeder K. (January 2003). Wi-Fi Handbook. New York, McGraw Hill professional.
- [15] Hiser, R., McCullough, Neely, A., Tucker, J., A. Wheat, J., & (2001). Designing a WirelessNetwork. Rockland, Syngress Publishing, Inc.
- [16] Dodd Z.A. (May 2002). The Essential Guide to Telecommunications. New Jersey, Prentice Hall PTR.
- [17] Yoshida, S. (January 1995). Propagation measurements and models for wireless communicationschannels, 42-49.
- [18] Sankar, K., Balinsky, A., Miller, D., Sundaralingam, S. (2005). Cisco Wireless LAN security. Indianapolis, Cisco Press.

- [19] Akyildiz, L.F., Martorell L.C., McNair J., Puigjaner R., and Yesha Y. (July 1999). Medium Access Control Protocols for Multimedia Traffic in Wireless Networks. IEEE Network, Vol. 13, 39-47.
- [20] Stallings, W. (1999). Cryptography And Network Security: Principles and practice. New Jersey, Prentice Hall.
- [21] Walker, J. (October 2000). Unsafe at any key size; an analysis of the WEP encapsulation, Intel Corporation, doc: 802.11/362.
- [22] Garcia A., Iwanchuk R., Schenk R. Wireless LAN deployment and Security Basics. Retrieved December 2005 from World Wide Web: <http://www.extremetech.com/article2/0,1697,1073,00.asp>
- [23] Vaughan S. 802.11 Vs. 3G. Retrieved December 2005 from the World Wide Web: <http://www.wi-fiplanet.com/tutorials/article.php/15775>
- [24] James, S. Building secure networks with DMZ. Retrieved July 2005 from World Wide Web: <http://neworder.box.sk/newsread.php?newsid=4817>
- [25] Lopez, J. (January 2005). WLANs vulnerable to hacking. News factor Technology news.
- [26] Molta, D. (January 2005). The state of Wireless Networking. Network Computing Magazine.
- [27] Calhoun, P. (September 2003). RADIUS (Remote Authentication Dial-In User Service) Support for Extensible Authentication Protocol (EAP), RFC 3579.

- [28] Hill, J. An analysis of RADIUS authentication protocol. Retrieved July 2005, from World Wide Web: <http://www.untruth.org/~josh/security/radius/radius-auth.html>
- [29] Microsoft Windows Server System. What is ISA Server? Retrieved February 18, 2005 from World Wide Web: <http://www.microsoft.com/isaserver/evaluation>
- [30] Redman: Microsoft Corporation. Security Hardening Guide: Microsoft Internet Security and Acceleration Server 2004. Retrieved March 7, 2005 from World Wide Web: <http://www.microsoft.com/isaserver/techinfo/Guidance/2004/configuration.mspx>
- [31] Microsoft Windows Server System. Using forwarders. Retrieved December, 2005 from the World Wide Web: <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/lcd13da9-ed0a-4814-b0bb-e46e8acle321.mspx>
- [32] Wanner, R., Securing your Linksys WRT54G. Retrieved: January 2005 from World Wide Web: http://www.whitehats.ca/main/members/Cerberus/secure_linksys_wrt54g/secure_linksys_wrt54g.html
- [33] Walrath J. D-Link High speed home networking. Retrieved December 2005 from World Wide Web: <http://www.penstarsys.com/reviews/network/dlink/hshn/>

APPENDIX - 1

- Screenshots of the RADIUS server configuration

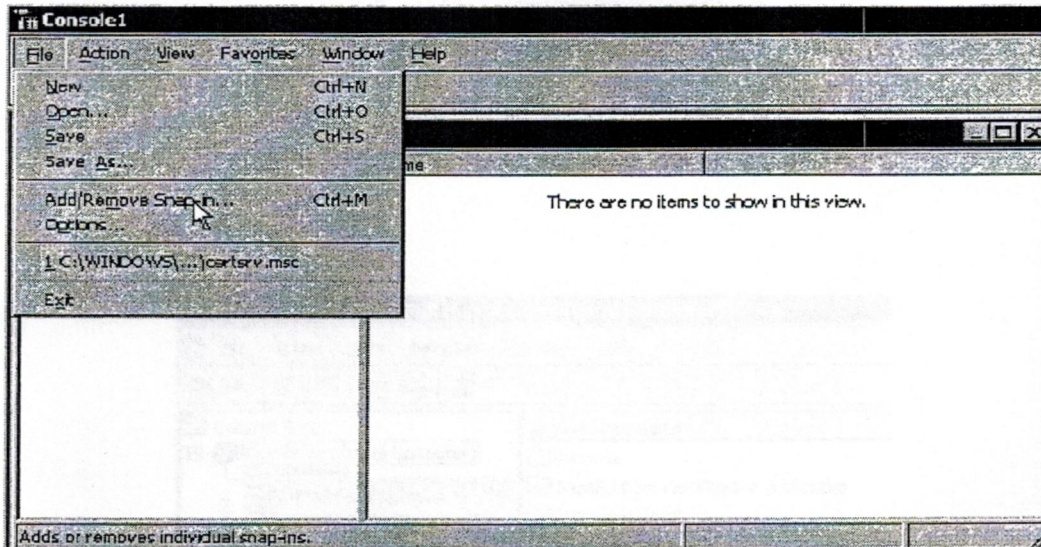


Figure A1.1 Installing Certificates for the Radius Server

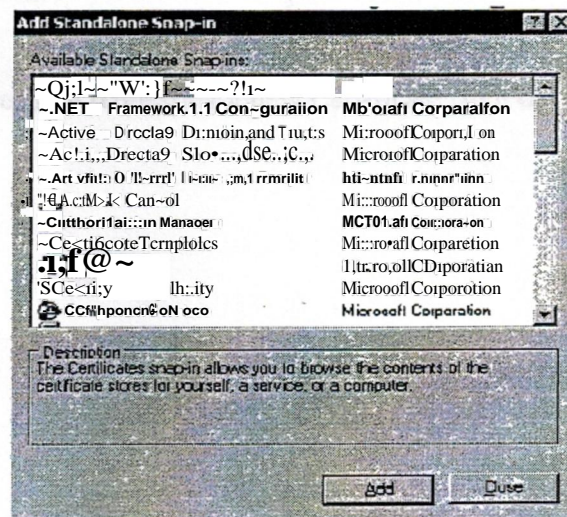


Figure A1.2 the contents of available certificates

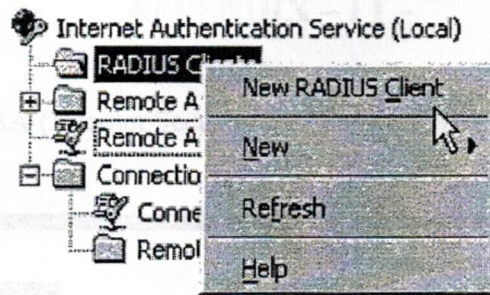


Figure A1.3 creating a Radius Client

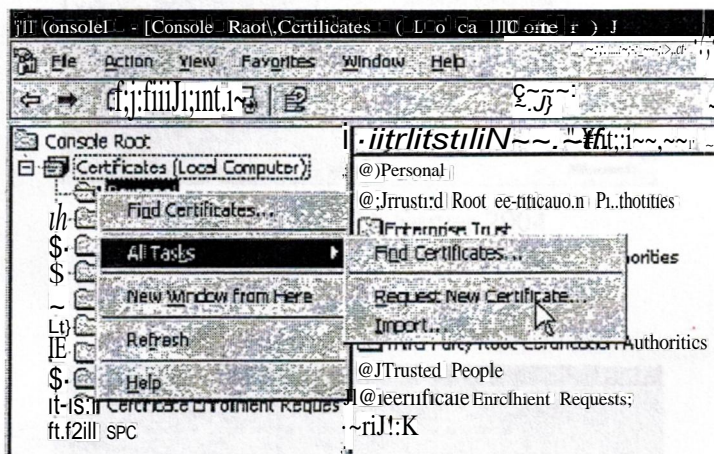


Figure A1.4 requesting a new Certificate from the console

APPENDIX - I I -

- Screenshots of ISA (Internet Security & Acceleration Server) 2004 configuration

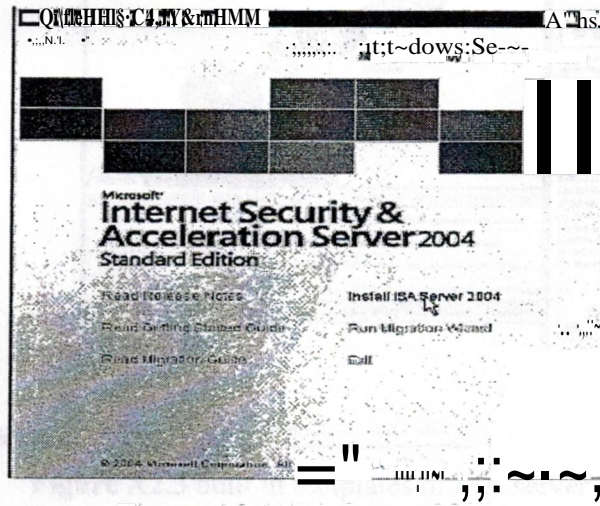


Figure A2.1 ISA Server 2004

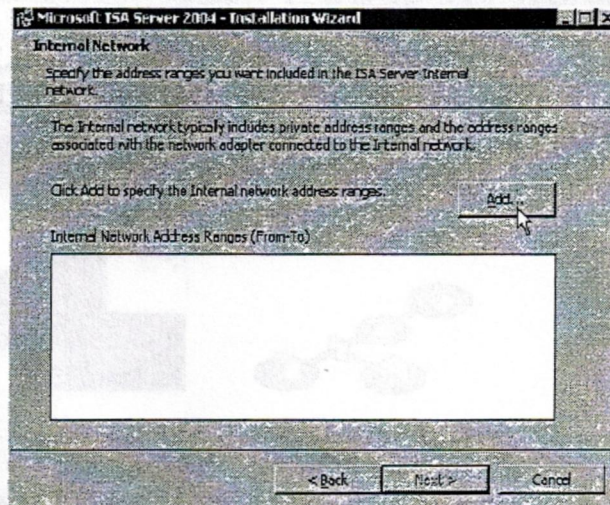


Figure A2.2 configuring the internal network of ISA

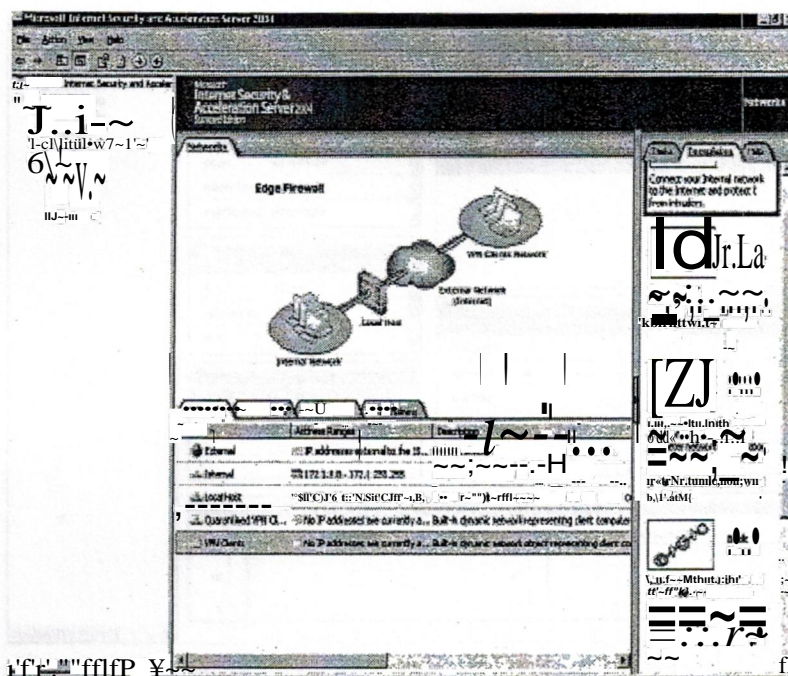


Figure A2.3 built in templates of ISA server

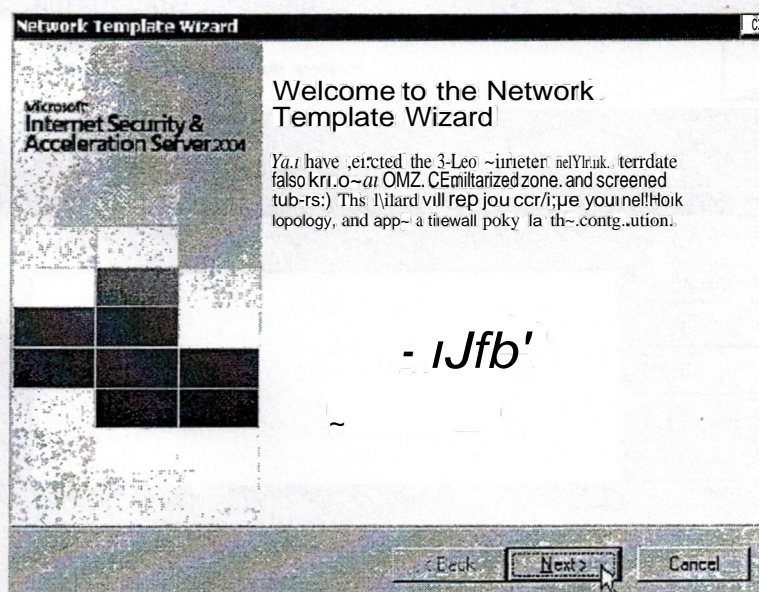


Figure A2.4 a 3-leg Perimeter

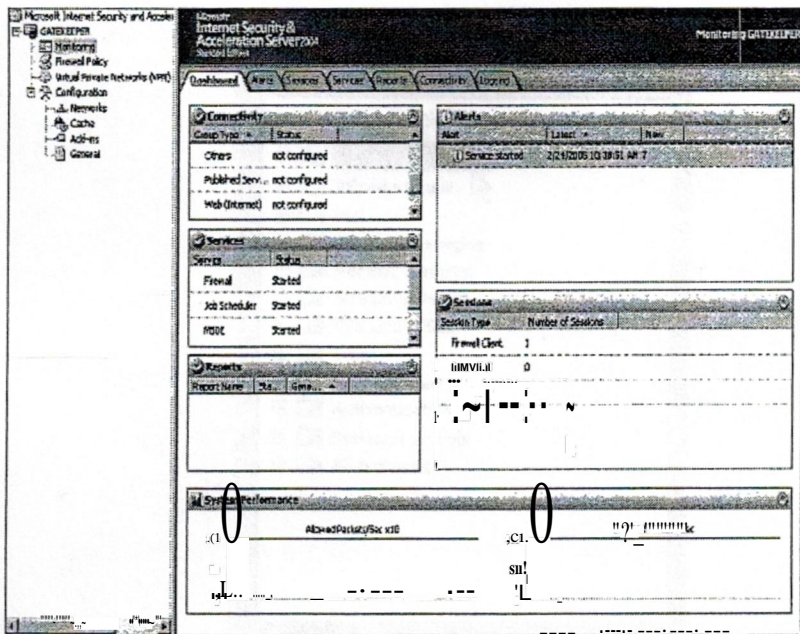


Figure A2.5 ISA server dashboard

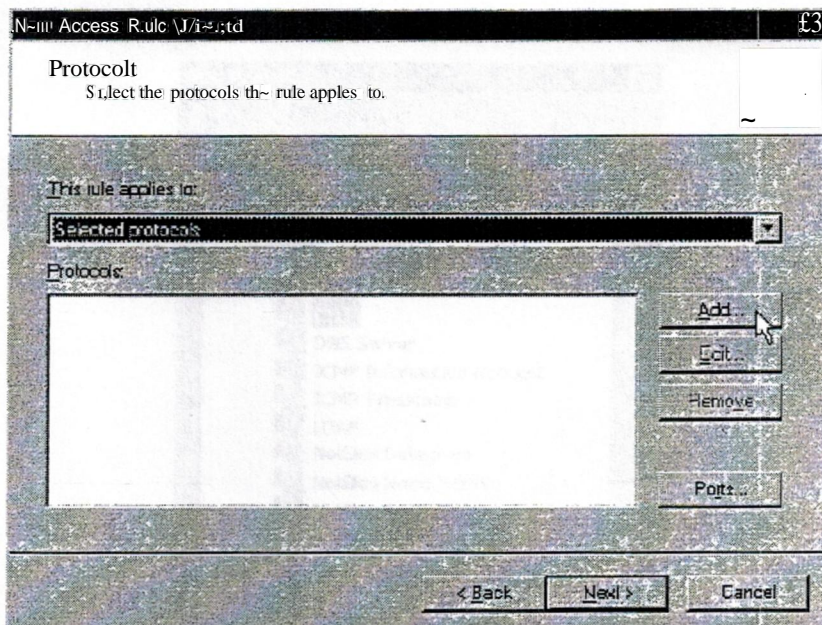


Figure A2.6 the name access rule wizard

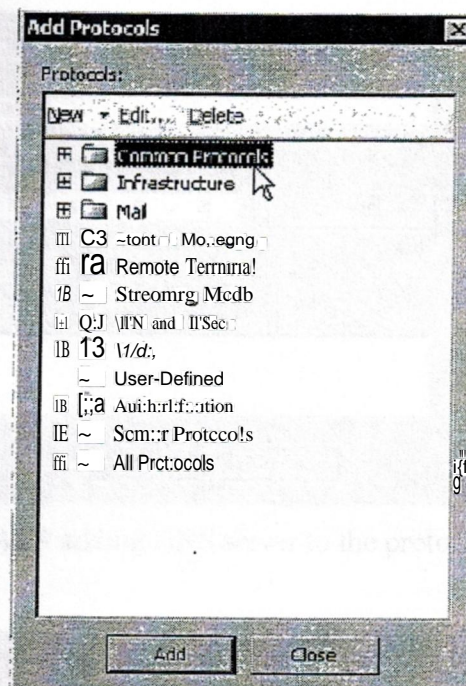


Figure A2.7 adding protocols to the wizard.

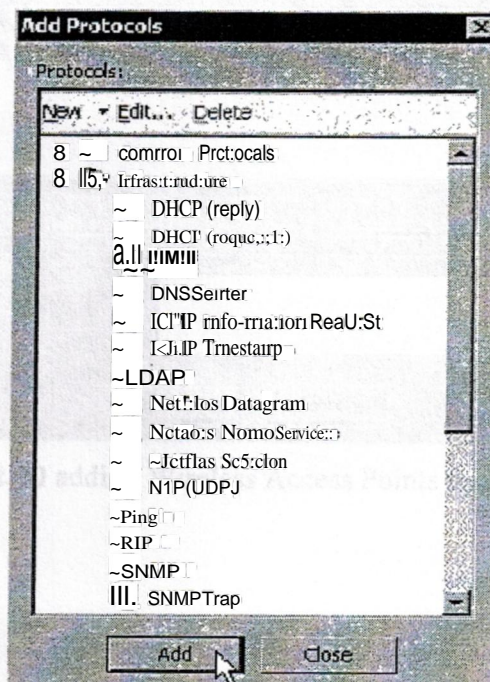
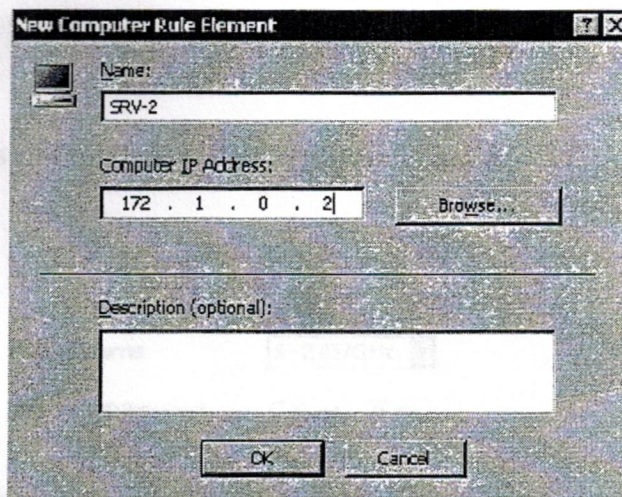


Figure A2.8 adding DNS protocol



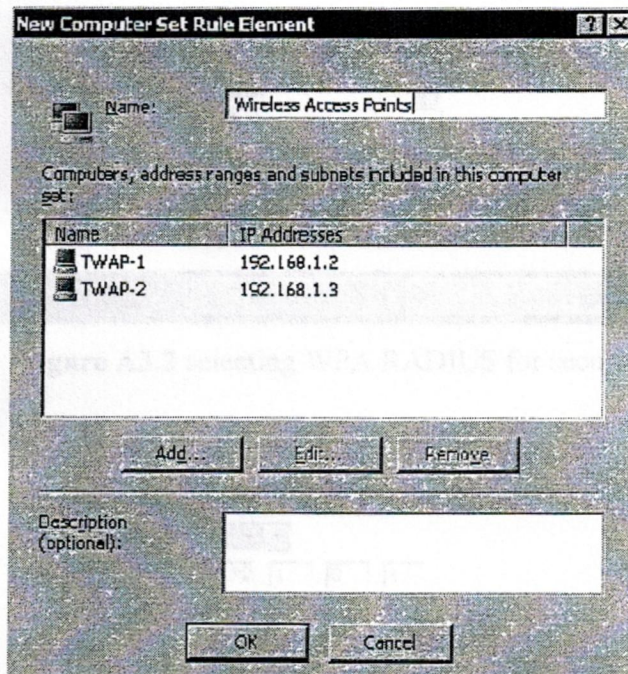
New Computer Rule Element

Name:

Computer IP Address:

Description (optional):



Figure A2.9 adding DNS server to the protocol



New Computer Set Rule Element

Name:

Computers, address ranges and subnets included in this computer set:

Name	IP Addresses
 TWAP-1	192.168.1.2
 TWAP-2	192.168.1.3

Description (optional):

Figure A2.10 adding Wireless Access Points to the protocol

APPENDIX- iii -

- Screenshots of a Linksys Access Point configuration

Wireless Mode: ☐ Network Mode: ☐ G-Only ☐ B ☐ G+N ☐ B+N

Wireless SSID:

Wireless SSID Broadcast: ☐ Enable ☒ Disable

Save Settings

Cancel Changes

Figure A3.1 configuring the Linksys for SSID and mode of transmission

Security Mode:

Disable
WPA Pre-Shared Key
WPA RADIUS
RADIUS
WEP

Save Settings

Cancel Changes

Figure A3.2 selecting WPA RADIUS for security

Security Mode:

WPA Algorithms:

RADIUS Server Address:

RADIUS Port:

Shared Key:

Key Renewal Interval:

Save Settings

Cancel Changes

Figure A3.3 entering information into the remaining fields

Advanced Routing

Opening Node

Dynamic Routing

Static Routing

RP: LAN & Wireless

Source: (Type remote) 3

Enter Remote Name: rtpoint

Destination LAN IP: 192.168.1.1

Subnet Mask: 255.255.255.0

Overan Gateway: 192.168.1.1

Interface: @ Wireless (b)

Show Routing Table

Figure A3.4 putting in advance routing information