**DOKUZ EYLÜL UNIVERSITY**
**GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES**

# MODELING AND DESIGNING WIRELESS NETWORKS FOR CORPORATIONS: SECURITY POLICIES AND RECONFIGURATION

**by**

**Ahmet Tuncay ERCAN**

**October, 2005**

**İZMİR**

# MODELING AND DESIGNING WIRELESS NETWORKS FOR CORPORATIONS: SECURITY POLICIES AND RECONFIGURATION

**A Thesis Submitted to the**
**Graduate School of Natural and Applied Sciences of Dokuz Eylül University**
**In Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy**
**in Computer Engineering, Computer Engineering Program**

**by**
**Ahmet Tuncay ERCAN**

**October, 2005**
**İZMİR**

**Ph.D. THESIS EXAMINATION RESULT FORM**

We have read the thesis entitled **"MODELING AND DESIGNING WIRELESS NETWORKS FOR CORPORATIONS: SECURITY POLICIES AND RECONFIGURATION"** completed by **Ahmet Tuncay ERCAN** under supervision of **Assoc.Prof.Dr. Yalçın ÇEBİ** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Doctor of Philosophy.

Assoc.Prof.Dr.Yalçın ÇEBİ

Supervisor

| | |
|---|---|
| Prof.Dr.Alp.R.KUT | Assoc.Prof.Dr.Birgül EGELİ |
| Committee Member | Committee Member |
| Asst.Prof.Dr.Zafer DİCLE | Asst.Prof.Dr.Gamze SEÇKİN |
| Jury Member | Jury Member |

Prof.Dr. Cahit HELVACI
Director
Graduate School of Natural and Applied Sciences

**ACKNOWLEDGMENTS**

First and foremost, I would like to express my deepest appreciation to my advisor, Assoc.Prof.Dr. Yalçın ÇEBİ, not only for his assistance and guidance, but also for the courses he taught. His supervisory style was an excellent match for me.

I would also thank Asst.Prof.Dr. Zafer DİCLE and Prof.Dr. Alp KUT to share their experience and expertise with me.

I owe my friends (Serden OZAKAR, Bora Kaan DALAY, Hayati ÇAM) and supporters in MoD, Turkey both past and present, for their outstanding help and participation in all phases of the related hardware and software design of the test environment. I would like to express my appreciation to my dear friend, Tarık ERSOY and Adem ÇETİN who provided network consulting and technical support for many of the products, wireless and wired network design assessments, and network security architecture.

Last, but most importantly, I wish to thank my parents (Necla and Serif ERCAN), and my loving wife, Nur. Her unfailing love, support, and companionship have made the process of writing and the long period of this thesis tolerable. When I have deeply felt uncertainty about the study, she has provided the encouragement to push on. I could not have reached this point without her, nor I can imagine a better soul with whom to face future challenges.

Ahmet Tuncay ERCAN

**MODELING AND DESIGNING WIRELESS NETWORKS FOR CORPORATIONS: SECURITY POLICIES AND RECONFIGURATION**

## ABSTRACT

This thesis gives an overview of fundamental wireless network information and wireless security issues. It provides a new point of view for successful wireless network setting that will be followed in the planning and implementing phases of critical Wireless Local Area Network (WLAN) systems, especially in the area of potential Military applications. We analyze the first implications of the network managers who will set up an official independent WLAN or a secondary wireless network as the extension of the currently used wired networks. Before the deployment of a new wireless network, a detailed project plan should be taken into consideration to figure out the pros and cons of the new architecture. After having the necessary information on Army requirements and constraints for WLANs, and discussing the implementation issues, a sample wireless network infrastructure model is validated according to the conditions written in the official directives. Next, a reasonable policy that can be followed up by the Army is presented for future use. This written document will help and lead network managers to follow up the future probable WLAN practices.

**Key Words:** Wireless networks, wireless standards, wireless security, requirements, constraints, wireless policy, multi-layer security.

# KURUMLAR İÇİN KABLOSUZ BİLGİSAYAR AĞLARININ MODELLEME VE TASARIMI: GÜVENLİK POLİTİKALARI VE YENİDEN KONFİGÜRASYONU

## ÖZ

Bu tez ile özellikle Silahlı Kuvvetler gibi görev ve kullanılan bilgi yönünden kritik sayılabilecek birimlerde tesis edilecek olan kablosuz yerel alan ağlarının, planlama ve projelendirme aşamalarında üzerinde durulması gereken temel hususlar açıklanmıştır. Mevcut kablolu ağların uzantısı olarak veya farklı bir bölgede ilk defa kurulacak olan kablosuz bir ağdan önce, ayrıntılı bir proje planı ele alınmalı ve yeni yapının kurulumu için zorunlu olan hususlar ortaya çıkarılmalıdır. Tespit edilecek bu bilgiler doğrultusunda resmi yönergelerde belirtilen koşullara uygun olarak örnek bir politika oluşturulacaktır. Kritik fonksiyonları olduğunu düşünen organizasyonlar bu politika ile ağ kullanım kararı öncesinde veya daha sonraki muhtemel kablosuz uygulamalarda doğru bir yol izleyebileceklerdir.

**Anahtar sözcükler:** Kablosuz bilgisayar ağları, kablosuz ağ standartları, kablosuz ağ güvenliği, gereksinimler, kısıtlar, kablosuz ağ politikası, çok-katmanlı güvenlik.

**CONTENTS**

**Page**

# CHAPTER ONE
# INTRODUCTION

## 1.1 General

Wireless LAN has become increasingly popular in recent years due to its advantages of simplicity and mobility. However, lots of WLAN deployments are also held back because of security concerns. When it is thought about connecting wireless devices into a mission-critical network system, such as Military and Private Networks, it is totally prohibited for a number of extremely serious risks, threats, and vulnerabilities associated with wireless communications.

The idea for this thesis is based on that the most important improvements in the 21st Century for Information Technologies are in the area of wireless systems. There is always a new story of a government or any other organization setting up a WLAN for public use. The most common thought for the users in either organizational or individual applications is whether wireless networks are adaptable to some criteria such as cheapness, portability, practicality, security, reliability, durability, and time saving. If it is thought what the wireless network means for an end user, the first issue that he/she will look for the answers is to learn what the mobile equipment can be and which applications can help him/her to use this network.

The purpose of this research is to build up a general model of Wireless LANs for corporations and find proper ways to implement it with the necessary security and configuration policies in the Army. Since Army is a mobile and deployable force, it requires both classified and unclassified data transfers over the wireless links. Therefore, integrating Wireless Local Area Networks (WLAN) to existing official wired network infrastructure could be beneficial to certain tactical military operations. Because it would decrease the time needed to set up, costs associated with laying wires, and manpower needs required to install, operate, and maintain the local area network (LAN).

With technological advances in WLAN communications, security and management, the existing threats and vulnerabilities may be mitigated to an acceptable level. In recent years, several researchers have studied the vulnerabilities present in the encryption protocols and authentication mechanisms associated with IEEE 802.11 based networks and the proactive management capabilities. These researches have led to the creation of protocol extensions and replacement proposals such as WPA, 802.11i, 802.1x, and suitable management tools for on-demand wireless LAN infrastructures.

### 1.2 Motivation

It shouldn't be neglected how important communications are, even though the utmost importance is water, food, and medical supplies. It may be seen wireless internet as a way to surf the net, download videos and music, conduct business, and just for plain fun. Communications of all sorts is very important. Those that are "missing" but still alive, who have no other way to communicate with loved ones all over the world, could mail their family to let them know their status.

Wireless Internet is probably the only viable means for rescue and relief workers to communicate when the cellular or the conventional telephony is down. Hospitals, shelters, relief agencies need to communicate with each other for disaster relief. Agencies in the devastated areas could use the Internet to communicate with their units in other countries, to order supplies, or to request what is needed. Additionally, in terms of tracking data and making informed decisions from command centers, Internet-transmitted information in the form of text, pictures, video, etc., is an effective tool than telephone.

Over the last century, advances in wireless technology have led to the radio, the television, the mobile telephone, and the communication satellites. All types of information can now be sent almost every corner of the world. Recently, a great deal of attention has been focused on satellite communication, wireless networking, and cellular technology.

Wireless LANs provide flexible installation, configuration and mobility in network environment. Key issues in implementing a wireless LAN are:

-Range and coverage,
-Throughput,
-Interoperability with wired infrastructure,
-Interoperability with wireless infrastructure,
-Interference and co-existence,
-Simplicity and ease of use,
-Security and Safety,
-Network management,
-Cost, Scalability,
-Battery life for mobile platforms.

Wireless systems have to be treated just like the wire net. Both nets require registration, and both nets need to know who and where you are and how you are accessing to them. If you are not a known entity, wired or wireless, you get shut down. A wireless LAN is not much more expensive than a wired LAN, and the maintenance costs are even lower. There is no other network solution that is more flexible, secure and easier to implement than the wireless LAN (Nichols, R.K., & Lekkas, P.C., 2002).

### 1.3 Problem Statement And Approach

Due to their characteristics, the wireless and mobile networks have much harder security requirement. Wireless communications can be more easily hacked than the wired networks. The other area where the security issues of the mobile environment are stressed, focuses at providing a seamless working environment for mobile users where the wireless network is as secure as the wired network to prevent security holes.

Even more than the traditional hardwired LANs, network security is an essential complement to IEEE 802.11 network connectivity. Because the traffic is transmitted over the radio and nobody has a direct control over who is listening or transmitting.

There are two major components of the Wi-Fi security problem. One is assuring the privacy of the data transmitted over the network against eavesdroppers. The other is protecting the network itself against intrusion. Unauthorized PCs may attempt to piggyback on the network, stealing bandwidth that is paid for. Even worse, unauthorized Access Points can be used to mount a variety of other dangerous attacks including listening to, diverting, or interrupting network traffic.

Finally, the goal of this thesis is to create official procedures for modeling and designing a WLAN for corporations with the proper security concerns and configuration techniques.

### 1.4 Overview And Style Of This Thesis

The security issues of wireless networks are different from the wired networks. The basic objective behind securing networks namely the confidentiality, non-repudiation and data integrity holds good respect to wireless as well. However, the dynamic environments make it more difficult to achieve security. This thesis gives a detailed look into various security schemes in wireless networks incorporated into wireless LAN standards, cryptographic and authentication protocols, and wireless applications and management functions.

The rising of Wi-Fi for home networks may raise security concerns for organizations. With the increase in telecommuting and consulting, IT managers need to be alert to the possibility that employees are transmitting sensitive data over unsecured networks. As a result, the employee’s home needs to be at least as secure as his office environment.

It is hoped that this paper will provide a valuable summary of wireless local area networks and introduce a possible wireless network policy and an architecture model. The plan of the thesis is considered as the following list:

Chapter 1 is an introduction to the subject, including a summary of historical information for wireless technology and networks. The chapter provides the basic effects of wireless systems.

Chapter 2 is devoted to a review of Wireless Networks. It concentrates on the general information about important wireless issues, namely wireless technologies, architecture, wireless network standards, and basic management systems.

Chapter 3 gives a typical overview of basic security issues that will be followed in the planning and implementing phases of critical WLAN systems especially in the area of potential Military applications. It includes fundamental security issues, concerns, and wireless security standards.

Chapter 4 examines wireless networks and the wireless infrastructures together with different aspects of wireless problems and solutions considered.

Chapter 5 describes a new approach to set up a wireless local area network model with the proper ways in an area and explain the common procedures for the companies that are willing to apply them. It begins with a set of guiding principles, and identifies the historical context from which the design borrows many facets. It then provides an overview of the major components of the design and presents each of them in turn. It mainly focuses on the security issues, the latest security protocols, and reconfiguration techniques for wireless devices. It analyzes the first implications from the point of network managers or CIS planners, to set up an official independent WLAN or as an extension of the currently used wired networks.

Chapter 6 represents a layered approach to Wireless LAN security concerns. It provides and overview of current security problems and reviews a general model of the applicable multi-level security policy.

Chapter 7 details the implementation of the sample application programs of a probable wireless LAN prototype for the army unit and the evaluation of it with the aforementioned policies. The chapter begins with these goals and then presents some technical details of the contents, and proceeds to describe the implementation of each basic component. It includes the description of the adaptive applications.

Chapter 8 concludes with a summary and identification of key contributions and main findings of this thesis and addresses the possible avenues of further research based on this work.

# CHAPTER TWO
# WIRELESS NETWORKS

## 2.1 Overview

Wireless Networks focus on networking and different user requirements like network architecture for personal communications systems, wireless LANs, radio, tactical, and other wireless systems (Rappaport, T.S., 1996). The demand will continue to grow in the new century.

A wireless system brings fundamental changes to networking. It uses electromagnetic airwaves (radio or infrared) to communicate from one point to another instead of cabling. Radio waves are often referred to as radio carriers, because they simply perform the function of delivering energy to a remote receiver. The data being transmitted is modulated on the radio carrier, so that it can be accurately extracted at the receiving end.

## 2.2 Wireless LAN Technologies

Wireless LANs employ radio frequency (RF) and infrared (IR) electromagnetic airwaves to transfer data from point to point. Table 2.1 below lists the frequency and wavelength numbers of the three wave types used in the wireless networking.

Table 2.1 Frequencies and Wavelength

| Wave Type | Frequency (Hz) | Wavelength (m) |
|---|---|---|
| Radio | $<1x10^{9}$ | $>1x10^{-1}$ |
| Microwave | $3x10^{9} – 3x10^{11}$ | $1x10^{-3} – 1x10^{-1}$ |
| Infrared | $3x10^{11} – 4x10^{14}$ | $7x10^{-7} – 1x10^{-3}$ |

The Federal Communications Commission (FCC) and a general world agreement set aside radio frequencies that are available for unlicensed commercial use. These

Industrial, Scientific and Medical (ISM) bands include the 900 MHz, 2.4 GHz, and 5 GHz bands that are used by many commercial wireless communication devices.

Several transmission mediums are capable of transferring data across airwaves. Each technology comes with its own set of advantages and limitations. Narrowband, wideband radio systems and Infrared systems are the leading technologies being used by the wireless industry.

### *2.2.1 Narrowband Technology*

A narrowband radio system transmits and receives user information on a specific radio frequency. It keeps the radio signal frequency as narrow as possible to pass the information. Undesirable crosstalk between channels is avoided by carefully assigning different users on different channel frequencies (Wireless LAN, 2004). In a radio system, privacy and noninterference are accomplished by using separate radio frequencies. The radio receiver filters out all radio signals except the designated frequency. A private telephone line is like a single radio frequency. When each home in a neighborhood has its own private telephone line, they can not listen the calls made in the other homes.

From a customer standpoint, one drawback of narrowband technology is that the end-user must obtain an FCC license for each site where it is employed.

### *2.2.2 Spread Spectrum Technology*

Most wireless LAN systems use the spread spectrum technology. Initiated from military technology, spread spectrum became the vital component for systems ranging from cellular to WLAN systems. More than a half century ago, the spread spectrum concept was introduced to solve the problem of reliable communications in the presence of intensive jamming (Marvin K.S., & Omura, J.K., 2001). It uses wideband, noise-like signals that are hard to detect. This technique spreads the signal over a wider band by spreading the code in both sides. This increases the bandwidth

of signals. The receiver should know the parameters of the band. If the receiver is not tuned to the right frequency, the signal looks like a background noise. There are two types of spread spectrum technology used in WLANs;

*2.2.2.1 Frequency Hopping Spread Spectrum (FHSS)*

FHSS uses a narrowband carrier that shifts frequency in a pattern known to both transmitter and receiver. This means that the frequency shifting spreads the transmission over a wide frequency band. When it is properly synchronized, it functions as a single logical channel. It appears to be a short-duration impulse noise to a receiver that doesn't know the hopping pattern.

The hopping sequence should try to avoid selection of adjacent cells. FHSS shows resistance to jamming unless the Jammer jams all frequencies. Collision in one or more frequencies can be recoverable. Spending the time to change the frequency introduces delay in transmission time. The FHSS systems are very cheap. Due to its limited ability to achieve higher data rates, the following techniques overtake the market shares.

*2.2.2.2 Direct Sequence Spread Spectrum (DSSS)*

In DSSS, a radio carrier is modulated by a digital signal. DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater is the probability that the original data can be recovered.

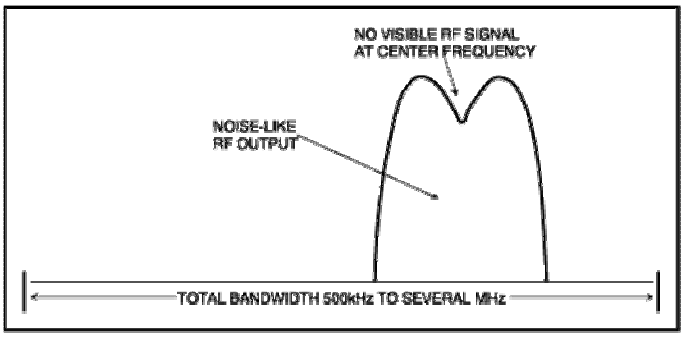


Figure 2.1 Direct Sequence Spread Spectrum

The disadvantage is that it requires more bandwidth (Figure 2.1). If one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. DSSS appears as low-power wideband noise and is rejected by most narrow band receivers to an unintended receiver.

The main problem with DSSS is the “Near-far effect”. This problem exists when an interfering transmitter is closer to the receiver than the original transmitter. The DSSS system also consumes more power than the FHSS system, since it is more complicated. On the other hand, the DSSS is more resistant to interference than FHSS. Transmission time in DSSS is shorter than FHSS, since it doesn’t wait to change the frequency.

#### *2.2.2.3 Orthogonal Frequency Division Multiplexing (OFDM)*

OFDM divides the allocated frequency range into sub-ranges that simultaneously transmit the pieces of the data stream. The more channels the system has, the more data can be transmitted in parallel, and the greater bandwidth can be achieved. Depending on the bandwidth requirements, OFDM may employ different modulation methods like phase-shift or amplitude-shift (Wireless Technology, 2003).

### *2.2.3 Infrared Technology (IR)*

The IR is another specification introduced by IEEE 802.11. Infrared transmission requires line of sight and is very susceptible to reflection. As a result, it has very low range and confined to a room, since the signals can not pass through the walls.

Infrared technology is rarely used in WLANs. IR systems use very high frequencies to carry data. IR cannot penetrate opaque objects. This limits the transmission capability to a direct line of sight or a diffuse method of communications. Diffuse communications alleviate the need for line of sight path. Transmission distance is limited in comparison with FHSS and DSSS

communications. Reflective IR wireless LAN systems do not require line-of-sight, but IR cells are limited to individual rooms. Inexpensive directed systems provide very limited range (1 m.) and typically are used for personal area networks, but occasionally are used in specific wireless LAN applications. It is already commonly used in remote control of TVs, VCD and DVD players. Infrared technology is also used and developed for remote control of environmental systems, personal computers and talking signs. High performance directed IR is impractical for mobile users and is therefore used only to implement fixed sub-networks (Krolak, M.K, & Novak, M.E., n.d).

## 2.3 Wireless LAN Contents

When we look at the devices used at the client side in a WLAN, they are not totally different from the ones in a regular wired network. The only differences are wireless devices, network adapters, Access Points, and Application Connectivity Software.

### *2.3.1 Wireless Devices*

Many types of computer devices operate on a wireless network (Figure 2.2). Users can adapt many existing computer devices to operate on a wireless network. Computer devices are often small to support mobile applications, and practical for people to carry with them.

Figure 2.2 Wireless Devices

### *2.3.2 Wireless Network Cards*

Each computer on the wireless network needs an adapter. The network interface card (NIC) provides the interface between the computer device and the wireless infrastructure. End users access the wireless LAN through these adapters which are implemented as PC cards. The NIC fits inside the computer device, but external network adapters are also available that plug in and remain outside the device. Wireless network interface cards come as PC cards, USB adapters, compact flash cards, or PCI cards.

A wireless NIC includes an antenna that converts electrical signals to radio or light waves for propagation through the air. Antennae employ many structures, and they can be external, internal, permanent, or detachable.

### *2.3.3 Access Points and Access Controllers*

Access points are the primary components in WLAN infrastructure (Figure 2.3). In a typical wireless LAN configuration, a transmitter/receiver (transceiver) device, called an access point, connects to the wired network from a fixed location using standard cabling. An access point represents a generic base station for wireless LAN. The 802.11 standard defines an access point as a communication hub for wireless users to connect to a wired distribution system. At a minimum, the access point receives, buffers, and transmits data between the wireless LAN and the wired network infrastructure. A single access point can support a small group of users and function within a range of less than one hundred to several hundred meters.

Figure 2.3 Access Points

A collection of access points within a WLAN, supports roaming throughout the facility. Access points also play a major role in providing better wireless security and control of users in a shared radio environment. In the absence of adequate security, quality of service, and roaming mechanisms in wireless network standards, companies offer access control solutions to strengthen wireless systems. The key component to these solutions is an access controller, which is typically hardware that resides on the wired portion of the network between the access points and the protected side of the network. Access controllers provide centralized intelligence behind the access points to regulate traffic between the open wireless network and important resources. In some cases, the access point contains the access control function.

### *2.3.4 Application Connectivity Software*

Each wireless device has an operating system. The operating system runs software needed to realize the wireless network application. In some cases, the operating system has built-in features that enhance wireless networks. For example, Windows XP has the ability to automatically identify and associate with WLANs. Moving between different network technologies and locations can be a problem for many users with mobile and wireless devices. Switching between Ethernet and WLAN connectivity requires a detailed setup of some configuration parameters.

Common applications like Web and e-mail perform very well on the wireless client device. Users may lose a wireless connection from time to time, but the protocols in use are always resilient. Beyond these applications, however, it will likely be necessary to incorporate connectivity software that provides an interface between a user's client device and the end system containing an application or database.

## 2.4 Wireless System Architecture

In many ways, 802.11 networking are very much like Ethernet networking (Figure 2.4). As seen in the figure, mobility is limited to the link layer. Network layer mobility is not generally available on the IP networks. The topology shown in the figure provides mobility between APs connected to the wired network backbone. All of the usual TCP/IP services, such as Domain Name Service (DNS), and Dynamic Host Configuration Protocol (DHCP) should also be provided in this network. Beyond considerations due to the physical environment, wireless networks often extend an existing wired infrastructure The wired infrastructure may be quite complex to begin with, especially if it spans several buildings in a campus setting.

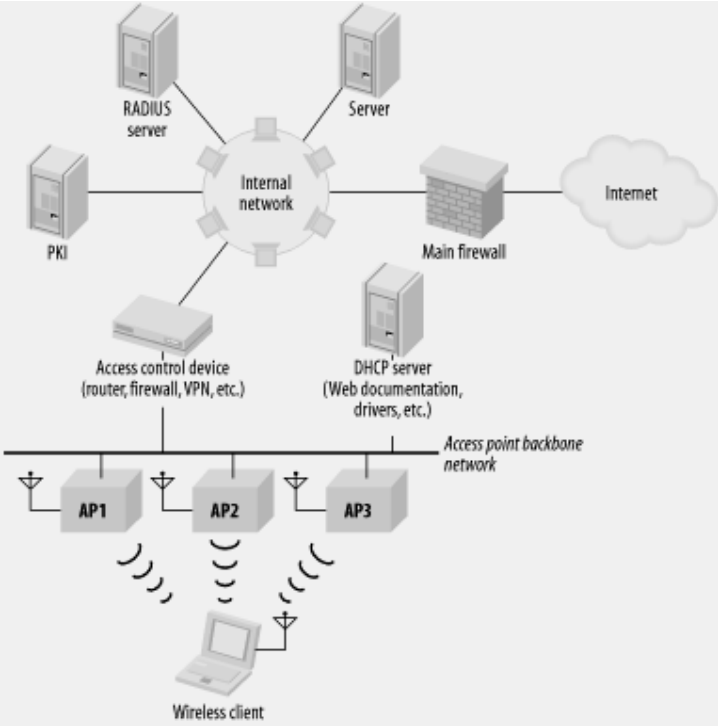


Figure 2.4 A sample Wireless Infrastructure

However, the current industry debates about the relative merits of a centralized WLAN architecture using WLAN switch (Figure 2.5) versus the more common distributed IEEE 802.11 access point architecture.

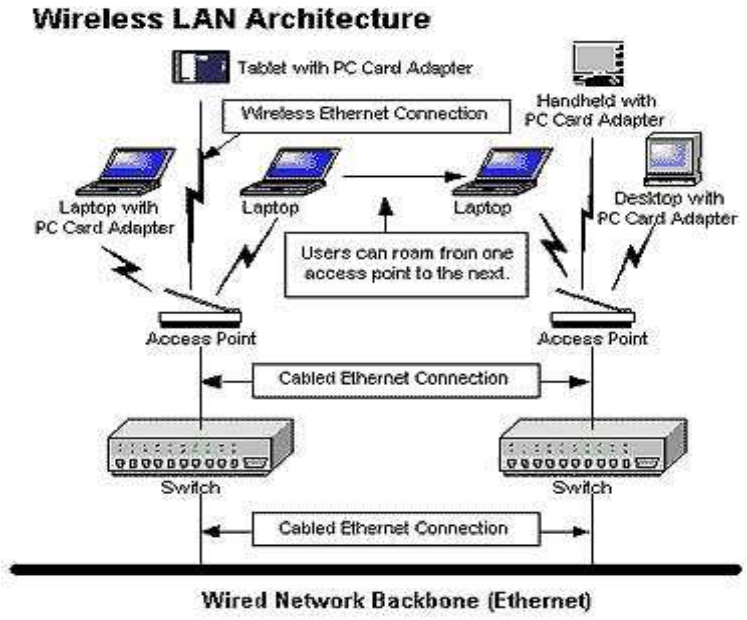


Figure 2.5 WLAN switch versus access point architecture

### *2.4.1 Infrastructure Mode*

Infrastructure mode wireless networking joins a wireless network to a wired Ethernet network. It also supports central connection points for wireless clients. Most of the wireless mobile computing applications today require single hop wireless connectivity to the wired network.

AP is required for infrastructure mode wireless networking. To join the WLAN, AP and all wireless clients must be configured to use the same network name. The AP is than cabled to the wired network to allow wireless clients access to the network, for example, Internet connections or printers. Additional APs can be added to the WLAN to increase the coverage of the infrastructure and support any number of wireless clients.

Infrastructure mode networks offer the advantage of scalability, centralized management of security and improved coverage. The disadvantage of infrastructure wireless networks is simply the additional cost to purchase AP hardware.

### *2.4.2 Ad Hoc Mode*

When there is no wired backbone infrastructure available for a group of mobile hosts or there also might be situations in which setting up fixed access points is not a viable solution due to cost, convenience, and performance considerations, an Ad Hoc network can be formed.

On wireless computer networks, ad hoc mode is a method for wireless devices to directly communicate with each other. Operating in this mode, allows all wireless devices within the range of each other to discover and communicate in peer-to-peer fashion without involving central access points. To set up an ad hoc network, each wireless adapter must be configured for ad hoc mode versus the alternative infrastructure mode. Ad hoc wireless networks eliminate the complexities of infrastructure setup and administration, enabling devices to create and join networks "on the fly" anywhere, anytime, for virtually any application.

In Ad hoc networks, each node is a mobile router equipped with a wireless transceiver. A node message goes to the other node that is in the transmission range of the first node or transferred between nodes that are indirectly connected via multiple hops through some other intermediate nodes. This is shown in Figure 2.6. Node C and node F are outside the wireless transmission range of each other, but still able to communicate via the intermediate node D in multiple hops (Craig, M., 2004).

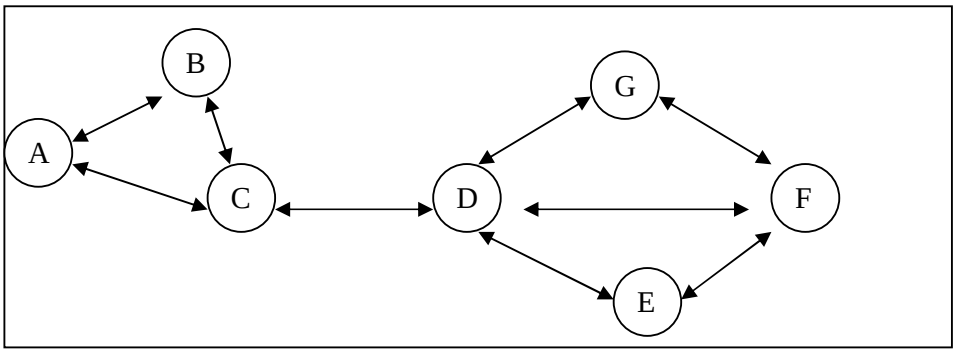


Figure 2.6 Basic structure of an ad hoc network

Ad Hoc Mobile Wireless Networks introduce detailed application scenarios ranging from home and car to office and battlefield. Applications of ad hoc networks

include military tactical communications, emergency relief operations, and commercial and educational use. The field is rapidly coming of age, reflecting powerful advances in protocols, systems, and real-world implementation experience.

#### *2.4.2.1 Mobile Ad hoc Networking (MANET)*

MANET is an autonomous collection of mobile users. The nodes are mobile and the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves.

Factors such as variable wireless link quality, propagation path loss, fading, multi user interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception (Mobile ad-hoc network, n.d).

## 2.5 Wireless LAN Standards

The standards are one of the important parts of the decision making involved in deploying a WLAN. Standards rarely introduce a new technology. Instead, they create common ways for a WLAN to be created, monitored, and managed. Vendors use the standards as a foundation and add unique or at least distinguishing features and functions to the standard.

Allocated frequency bands for wireless LAN applications are typically in 2.4 GHz and 5 GHz ranges where the bandwidth is scarce and in much demand. WLAN system at 2.4 GHz must meet ISM (Industrial, Scientific and Medical) band

requirements. The IEEE 802.11 standard supports both FHSS and DSSS techniques for this band.

Table 2.2 helps to differentiate between the available wireless networking standards and choose which standard might be the right fit for the organization.

Table 2.2 Wireless LAN Standards

| Standard | Data Rate | Frequency | Modulation |
|---|---|---|---|
| IEEE 802.11 | up to 2 Mbps | 2.4 GHz | FHSS or DSSS |
| IEEE 802.11a | up to 54 Mbps | 5 GHz | OFDM |
| IEEE 802.11b | up to 11 Mbps | 2.4 GHz | DSSS |
| IEEE 802.11g | up to 54 Mbps | 2.4 GHz | DSSS or OFDM |
| Bluetooth | up to 2 Mbps | 2.4 GHz | FHSS |
| HomeRF | up to 10 Mbps | 2.4 GHz | FHSS |
| HiperLAN/1 | up to 20 Mbps | 5 GHz | CSMA/CA |
| HiperLAN/2 | up to 54 Mbps | 5 GHz | OFDM |

### *2.5.1 802.11*

802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The bandwidth of 802.11 is 1 or 2 Mbps and operates at 2.4 GHz band using FHSS or DSSS. The IEEE accepted the specification in 1997.

The advantages of a 2.4 GHz wireless network include a higher data rate and it's an Institute of Electrical and Electronics Engineers (IEEE) open standard-enabling mobile devices to communicate with a wired network and run any software, just like an ordinary workstation. 2.4 GHz wireless LAN is the proper technical foundation for the future. It allows remote computers to use a Graphical User Interface (GUI), transfer files and can support emerging Voice-over-IP (VoIP) technology.

### *2.5.2 802.11b*

Wireless LAN technology standard 802.11b has the strongest momentum to becoming the main standard for corporate internal wireless LAN networks. The bandwidth of 802.11b is 11 Mbps and operates at 2.4 GHz Frequency. 802.11b was 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.

802.11b specifies the High Rate extension of the PHY for the DSSS system in 2.4 GHz band designated for ISM applications. This extension of the DSSS system provides 5.5 Mbps and 11 Mbps payload data rates. To provide the higher rates, 8-chip complementary code keying (CCK) is employed as the modulation scheme together with DSSS (IEEE Std. 802.11b, 1999).

### *2.5.3 802.11a*

The successor of the current 802.11b standard is 802.11a and is designed to be faster and operate at a different frequency. IEEE 802.11a has been developed to provide high data rate service at 5 GHz U-NII bands. IEEE 802.11a selects multi-carrier modulation. Multi-carrier modulation is a strong candidate for packet switched wireless applications and offers several advantages over single carrier approaches. The OFDM system is a viable solution to accommodating 6-54 Mbps data rates.

802.11a specifies the Physical Layer entity for an OFDM system and the additions that have to be made to the base standard IEEE 802.11 to accommodate the OFDM PHY. It runs in 5 GHz band, free from the crowded 2,4 GHz band used by 802.11b and g (and microwave ovens and Bluetooth). However, it is mainly used in U.S, since the band generally are used by Civilian Organizations in Europe. The OFDM system provides a wireless LAN with data payload communication capabilities of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps (IEEE Std. 802.11a, 1999).

802.11a quietly is gaining ground as a wireless LAN standard of choice. At sites where these deployments are unfolding, users say 802.11a delivers two critical advantages with its added capacity and lack of interference (Singh, S., 1996). It offers 12 to 24 radio channels instead of 802.11b and g's three channels, so far more throughput to many users can be given. When 802.11a products emerged in 2001, early products had range problems and were more expensive than 802.11g or b products. However, 802.11a users say the added capacity and lack of interference are worth the extra money.

Faced with an array of network infrastructure needs an end-user demand, network executives are adding 802.11a technology to older WLANs or deploying from scratch wireless networks that can support the 54Mbps 802.11a and g and the older 11Mbps 802.11b.

A company can choose to overlay 802.11a on an 802.11b network or go with 802.11a/g for brand-new networks. They are future-proofing themselves. While some organizations with 802.11b or even 802.11g might discourage big file transfers, others are turning to 11a as a means of making WLANs ever more capable. They run with streaming video now (It is just like a TV, you walk all around campus and watch TV on the notebook).

### *2.5.4 802.11g*

802.11g is a new physical layer within the IEEE 802.11 standard family. 802.11g specifies further rate extension of the PHY for the DSSS system. This is known as the Extended Rate PHY (ERP) and operates in the 2.4 GHz ISM band. Data rates are 1, 2, 5.5, and 11 Mbps. 802.11g provides additional payload data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps (Molnar, D., 2003). It joins IEEE 802.11b that has achieved enormous success in the marketplace, and the lesser known but higher performance IEEE 802.11a (Craig, M., 2004). In addition, in fact, 802.11g will be completely backwards compatible with 802.11b.

It will work with the existing 802.11 MAC (medium access control layer) and all of the proposed enhancements for 802.11, like 802.11i, which will have improved security. Moreover, all other network operating system features which are looked for file transfers will still be available in the 802.11g standard. There are wide varieties of 802.11g infrastructure products, including those that are aimed at the enterprise market. The Wi-Fi Alliance, which certifies interoperability, will have a chance to do that with 802.11g products.

If there is an access point with 11g, and there is one computer connected to it with 11b, then everyone else on that access point has to run at the 11b rate. If the access points are on the same channel, interference occurs.

### *2.5.5 Problems with 802.11*

Enterprise users rarely ran into bandwidth problems, capacity issues, or radio channel conflicts, because 802.11b and then 802.11b/g WLAN deployments tend to be relatively small,. More users are wireless, applications are more demanding and the executives are considering adding VoIP to their WLANs. As a result, WLAN infrastructures are being designed with both frequency bands in mind, and sometimes all three WLAN standards.

Aside from complex software and hardware issues, lack of a uniform wireless protocol in the U.S. is hampering product development and making compatibility difficult if not impossible. Wireless industry standards could emerge within the next year, in time to support third-generation (3G) wireless product development.

### *2.5.6 HiperLAN/2*

HiperLAN/2,which stands for High Performance Radio Local Area Network, is a wireless LAN standard. HiperLAN/2 defines a very efficient, high-speed wireless LAN technology that fully meets the requirements of Europe’s spectrum regulatory. Similar to IEEE 802.11a, HiperLAN/2 operates in the 5 GHz frequency band using

OFDM and offers data rates of up to 54 Mbps. In fact, the physical layer of HiperLAN/2 is very similar to the one that 802.11a defines.

#### *2.5.6.1 Basic Differences*

The similarities between 802.11a and HiperLAN/2 stop at the MAC layer. While 802.11a uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) to transmit packets, HiperLAN/2 uses TDMA (Time Division Multiple Access). The use of TDMA offers a regular time relationship for network access. TDMA systems dynamically assign each station a time slot based on the station's need for throughput. The stations then transmit at regular intervals during their respective time slots, making more efficiently use of the medium and improving support of voice and video applications.

#### *2.5.6.2 HiperLAN/2 Features*

HiperLAN/2 has a number of attractive features as compared to 802.11. The first, and probably most important, is higher throughput. It also implements quality of service protocols for different sorts of connections. This allows HiperLAN/2 to support the transmission of data, video, and voice. A unique feature of HiperLAN/2 technology is the ability to interface with other high-speed networks, including 3G cellular, ATM (Asynchronous Transfer Mode), and other Internet protocol based networks. This is a real advantage when integrating Wireless LANs with cellular systems and wide area networks (Geier, J., 2003).

### *2.5.7 Bluetooth*

Bluetooth is a wireless personal area-networking (WPAN) standard. Its goal is to enable users to connect many different computing and telecommunications devices easily and simply, without the cables. It operates in the unlicensed 2.4 GHz band of radio spectrum. Its range is too short and its throughput speed is too low (1Mbps).

Bluetooth devices can coexist peacefully and in some cases interoperate with Wi-Fi network (Wireless technology, 2005).

Bluetooth connects peripherals without cables. Keyboards, optical mice, printers, digital cameras, and PDAs that employ Bluetooth are already available. All of these devices can communicate and operate without user intervention.

### *2.5.8 Metropolitan Area Network /WiMAX*

WiMAX is a wireless networking standard (based on IEEE 802.16 wireless broadband standard specification) that provides high-throughput broadband connections over long distances. WiMAX will transfer data at about 70 Mbps over a distance of 30 miles to thousand of users from a base station. WiMAX technology is about to revolutionize the broadband wireless Internet access industry. It can be used for a number of applications, including “last mile” broadband connections, hotspots, and cellular backhaul, and high-speed enterprise connectivity (such as DSL, T1/E1) for business (WiMAX in Action, n.d).

## 2.6 Management Systems

Wireless LANs are just like other LANs, except that the connection. This implies that managing a wireless LAN shouldn’t be different from managing a wired LAN. Such matters as traffic monitoring, user throughput, and security are managed in the wireless domain just as they are on wire (Craig, M., 2004).

However, wireless introduces a number of other interesting problems and challenges. First, wireless network performance is becoming more and more important for enterprises deploying business-critical wireless networks. As the networks grow in size and become an integral part of our daily life, throughput intensive applications like voice over WLAN, content delivery are also gaining popularity. In such applications, where network throughput performance is critical, detailed network planning, monitoring, and management become essential. Network

planning includes detailed site surveys, determining the number of access points, locations, AP configurations.

### *2.6.1 Airwave Management*

Airwave management deal specifically with the wireless part of a wireless LAN. Capabilities like monitoring for unauthorized users, denial of service attacks, and rogue APs are included. Airwave management tools are often implemented as software in notebook computers or even PDAs, and are fundamentally ad-hoc in nature. It's also possible to use tools called network analyzers or spectrum analyzers to look at the energy present in the air at specific frequencies in specific locations, independent of WLAN (and other) protocols. These devices can be useful in debugging interference-related problems and other issues related to radio propagation.

### *2.6.2 WLAN Management*

This is the set of capabilities usually provided with a WLAN product or a third-party WLAN management tool. It is implemented in software that runs on a server or appliance. User management, monitoring, and security policy definition and execution, are included among other functions. It is thought that WLAN management will eventually contain many of the airwave management tools, as APs and air monitors.

### *2.6.3 Network Management*

This is the functionality included in large-scale network-management tools, like HP's OpenView, and Micromuse's NetCool., IBM's Tivoli and CA's Unicenter. These products have many features for the WLAN management. They are further motivated by customer demands for more integrated network and WLAN management features.

# CHAPTER THREE
# WIRELESS SECURITY

## 3.1 Introduction

An increasing number of government agencies, businesses, and home users are using or at least considering using wireless technologies in their environments. Agencies should be aware of the security risks associated with wireless technologies. A WLAN is different from a wired LAN, in the fact that RF waves travel through physical barriers that enter into the public domain, which are now accessible by anyone. There is not a clear violation of the company's property rights, if the WLAN is locked down to prevent open authentication. Strategies need to be developed in order to mitigate risks as wireless technologies are integrated into their computing environments.

The flexibility and mobility of wireless LAN technology can deliver significant advantages. Because WLAN technology is based on radio wave transmissions, it has provoked legitimate concerns about network security. The further widespread deployment of WLANs depends on whether secure networking can be achieved. In order for critical data and services to be delivered over WLANs, a reasonable level of security must be guaranteed. Both network access and data protection issues known as authentication and encryption need to be addressed (Molnar, D., 2003) to protect a wireless LAN network,

Wireless technology, by its nature, violates fundamental security principles. It does not ensure the identity of the user and the device (authentication), nor prevent the sender of the message from denying he or she has sent (non repudiation) (Nichols, R.K., & Lekkas, P.C., 2002).

In the corporate world, it is unthinkable to implement an IT strategy without a significant emphasis on security. Faced with a highly competitive business environment, enterprises are under great pressure to ensure the security of a broad

range of both internal and external information. These enterprises face potentially crippling loss if information such as personal communications, personal records, and customer data and more importantly Government or Military based data is inappropriately changed, accessed, or stolen.

802.11 networks have unique vulnerabilities. Wireless networks cannot be physically secured the same way a wired network can be. An attack against a wireless network can take place anywhere: from the next office, the parking lot of the building, or across the street in the park.

Understanding the details of various attacks against the wireless infrastructure is critical to determining how to defend the network. Some attacks are easy to implement but aren't particularly dangerous. Other attacks are much more difficult to mount but can be devastating. Like any other aspect of security, wireless security is a game of risk. By knowing, the risks involved in the network and making informed decisions about security measures, you have a better chance at protecting yourself, your assets, and your users (Potter, B., & Fleck, B., 2002).

## 3.2 Basic Security Issues

As more wireless technology is developed and implemented, the complexity of types of the attacks will increase. These attacks may be very similar against other wireless type technologies and is not unique to 802.11b,a or g. By understanding these risks and how to develop security solution for 802.11 overall, it will be a good stepping-stone for providing a good security solution to any wireless problem.

### *3.2.1 Authentication and Authorization*

The two main goals of wireless LAN security planning are ensuring adequate access control and preserving the confidentiality of data, as it traverses the wireless network. Security requirements may be dictated by legal requirements or the legal threat of unauthorized data disclosure.

Authentication has long been a weak point of 802.11 networks. The two main options provided by 802.11 are to filter on the Media Access Control (MAC) addresses of wireless stations allowed to connect or use shared Wired Equivalent Privacy (WEP) keys for stronger authentication. In practice, MAC address filtering is too cumbersome and error-prone, so the choices are to use WEP authentication or depend on external solutions. Authentication for an extranet should always tie identity to an individual, not a machine or IP address. User-based authentication ranges from simple passwords on the low end to complex biometrics at the high end. Most companies today are deploying some form of two-factor authentication, which means something the user has and something the user knows, such as a token card and PIN.

### *3.2.2 Encryption*

Data confidentiality is provided by encryption services. One option is the WEP standard, though higher-security sites may opt for additional VPN technology on top of the 802.11 layers.

Because encryption can affect performance, turning the encryption off when it is not required can be useful. However, any information that are confidential (patient records, research, personal account data, etc.) should always be encrypted. The longer the key length of the cryptographic algorithm, the stronger is the encryption. Today, 168-bit 3DES is the strongest commercially available key length in the United States and other European countries. Nevertheless, there are legal limits on the strength of the encryption that can be exported. Until this issue is resolved, companies should look for extranet solutions that can offer multiple levels of encryption.

### *3.2.3 Integrity*

Data integrity issues in wireless networks are similar to those in wired networks. Because organizations frequently implement wireless and wired communications

without adequate cryptographic protection of data, integrity can be difficult to achieve. A hacker, for example, can compromise data integrity by deleting or modifying the data in an email from an account on the wireless system.

Other kinds of active attacks that compromise system integrity are possible, because the existing security features of 802.11 standard do not provide for strong message integrity. Message modification attacks are possible when cryptographic checking mechanisms such as message authentication codes and hashes are not used.

## 3.3 Wireless Security Concerns

In addition to knowing which devices are in use, enterprises must understand their specific capabilities and hardware/software characteristics. Key elements include:

- How might mobile devices connect to elements of the enterprise technology infrastructure?
- What capabilities exist on the devices for application execution?
- What capabilities exist on the devices for email reception and attachment storage?
- What level of security is currently built into the devices (e.g. encryption, password protection, remote disablement)?

### *3.3.1 Infrastructure Mode Wireless Security*

The specifications for the protocols of 802.11a are very similar to 802.11b; therefore many of the security risks are shared for both 802.11a and 802.11b. Many of the security issues around 802.11b will continue to be an issue with 802.11a, therefore by understanding current issues will help organizations deal with future issues as well. The default configuration of wireless access points do not have any security features turned on.

*Service Set Identifier (SSID)* is a simple password that identifies the WLAN. Clients must be configured with the correct SSID to access their WLAN.

*MAC* address filtering restricts WLAN access to computers that are on a list created for each access point of the WLAN.

*WEP* is an encryption scheme that protects WLAN data streams between clients and access points (AP) as specified by the 802.11 standard.

### *3.3.2 Ad Hoc Mode Wireless Security*

In ad hoc wireless networks the communicating nodes do not rely on a fixed infrastructure, which sets new challenges for the necessary security architecture they apply. In addition, as ad hoc networks are often designed for specific environments and may have to operate with full availability even in difficult conditions, security solutions applied in traditional networks may not be directly suitable for protecting them. Anybody can easily hack the network by sniffing the packets that are broadcasted that also leads to eavesdropping and interception. Apart from these security hazards there are a few security problems that are in particular more common in wireless networks.

The ad hoc model is naturally attack prone, because of both the hardware limitation and communication media. The hardware limitation poses tight constraints on both communication and computing power.

## 3.4 Wireless Security Standards

Organizations should be aware that maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems. Moreover, it is important that agencies assess risks more frequently, and evaluate system security controls when wireless technologies are deployed.

### *3.4.1 Wired Equivalent Privacy (WEP)*

WEP is an encryption algorithm used by shared Key authentication process for authenticating users and for encrypting data payloads over only the wireless segment of the LAN. The IEEE 802.11 standard specifies the use of WEP. It was intended to provide “confidentiality” that is equivalent to the confidentiality of a wired local area network that does not employ cryptographic techniques. IEEE specifications for wired LANs do not include data encryption as a requirement. This is because all of these LANs are secured by physical means such as walled structures and controlled entrance to buildings, etc. However, no such physical boundaries can be provided in case of WLANs, thus justifying the need for an encryption mechanism (The formal WEP specification, n.d).

WEP is a simple algorithm that utilizes a pseudo-random number generator (PRNG) and the RC4 stream cipher. RC4 stream cipher is fast to decrypt and encrypt, which saves on CPU cycles. RC4 is also simple enough for most software developers to code it into software.

When WEP is referred to as being simple, it means that it is weak. The RC4 algorithm was inappropriately implemented in WEP, yielding a less-than-adequate security solution for 802.11 networks. Both 64-bit and 128-bit WEP have the same weak implementation of a 24-bit Initialization Vector (IV) and use the same flawed process of encryption. The flawed process is that most implementations of WEP initialize hardware using an IV of 0 (zero), and there after incrementing the IV by 1 (one) for each packet sent. For a busy network, statistical analysis shows that all possible IVs ($2^{24}$) would be exhausted in half a day, meaning the IV would be reinitialized starting at zero at least once a day. This scenario creates an open door for determined hackers.

### *3.4.2 IEEE 802.1x and Extensible Authentication Protocol (EAP)*

This is an IEEE standard that addresses WEP security flaws. This was widely implemented in the late 2001 and throughout 2002 by wireless LAN. 802.1x is an IEEE port-based authentication standard that works to provide authentication for both wired and wireless LANs. For a WLAN environment, 802.1x provides dynamic keys instead of the static keys used in WEP authentication. This clearly improves security for WLANs (Molnar, D., 2003).

The 802.1x protocol has been incorporated into many wireless LAN systems and has become almost a standard practice among many vendors. When combined with EAP, 802.1x can provide a very secure and flexible environment based on various authentication schemes in use today.

EAP, which was first defined for the point-to-point protocol (PPP), is a protocol for negotiating an authentication method. EAP is defined in RFC 2284 and defines the characteristics of the authentication method including the required user credentials (password, certificate, etc.), protocols and the support of mutual authentication. Neither the industry players nor IEEE have come together to agree on any single type of a standard. There are still many types of EAP currently on the market.

### *3.4.3 Temporal Key Integrity Protocol (TKIP)*

TKIP is essentially an upgrade to WEP that fixes known security problems in WEP's implementation of the RC4 stream cipher. TKIP provides for initialization vector hashing to help defeat passive packet snooping. It also provides a Message Integrity Check to help determine whether an unauthorized user have modified packets by injecting traffic that enables key cracking. TKIP includes use of dynamic keys to defeat capture of passive keys- a widely publicized hole in existing WEP standard.

### *3.4.4 Wi-Fi Protected Access (WPA)*

Over the past years, many “Wi-Fi Alliance” members and their customers have become increasingly concerned about the vulnerabilities of WEP, the basic mechanism to date for interoperable security in Wi-Fi Certified products. In response, the Wi-Fi Alliance in conjunction with the IEEE, has driven an effort to bring strongly enhanced, interoperable Wi-Fi security namely WPA to market in the first quarter of 2003. WPA is a response by the WLAN industry to offer an immediate, strong security solution. WPA not only provides strong data encryption but also adds user authentication to correct WEP weaknesses. It is being deployed in wireless LAN products as a standard feature, and vendors are making this protection available with a software download.

WPA is a specification of standard-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. Designed to run on existing hardware as a software upgrade, WPA is derived from and will be forwarded being compatible with the IEEE 802.11i standard. The Wi-Fi Alliance has taken a subset of the draft 802.11i standard, calling it WPA, and now certifies devices that meet the requirements. When properly installed, it will provide WLAN users with a high level of assurance that their data will remain protected and that only authorized network users can access the network.

WPA uses TKIP as the protocol and algorithm to improve security of keys used with WEP. While WPA goes a long way toward addressing the shortcomings of WEP, not all users will be able to take advantage of it. That's because WPA might not be backward compatible with some legacy devices and operating systems. What's more, TKIP/WPA will degrade performance unless a WLAN system has hardware that will run and accelerate the WPA protocol. Moreover, not all users can share the same security infrastructure. Some users will have a PDA and lack the processing resources of a PC. For most WLANs, there's currently a trade-off between security and performance without the presence of hardware acceleration in the access point.

### *3.4.5 802.11i*

The IEEE formally approved the long awaited 802.11i extension to the 802.11 wireless LAN standard for more robust security. The Wi-Fi Alliance began vendor product certification testing in September 2004. 802.11i is building the standard around 802.1x port-based authentication for user and device authentication. The 802.11i standard includes two main developments: Wi-Fi Protected Access (WPA) and Robust Security Network (RSN) (Cohen & O'hara, 2003).

Most portions of 802.11i, informally known as WPA, are already at work in products. WPA, for example, requires products to rotate encryption keys on a per-packet basis and use the industry standard 802.1x framework for authentication. Preauthentication benefits security and performance. A scheme called "Pairwise Master Key (PMK) Caching" sets up a shared key between a client device and its authenticator".

When a client roams between access points, the client's credentials no longer must be completely reauthenticated which is a task that can take more than 100 milliseconds. In the case of a voice session, for example, a connection would likely be dropped if handoff were to take this long. Historically, WLANs could support fast or secure roaming, but not both. Over time, many vendors have come up with proprietary ways of achieving both capabilities. Now there 's a standard for doing so. The preauthentication scheme comes into play when users roam and in cases when signal strength fades and a client needs to find another access point with which to associate.

#### *3.4.5.1 Robust Security Network (RSN)*

RSN uses dynamic negotiation of authentication and encryption algorithms between access points and mobile devices. The authentication schemes proposed in the draft standard are based on 802.1x and EAP. The encryption algorithm is Advanced Encryption Standard (AES). Dynamic negotiation of authentication and

encryption algorithms let RSN evolve with the state of the art in security, adding algorithms to address new threats and continuing to provide the security necessary to protect WLAN information.

Using dynamic negotiation, 802.1x, EAP, and AES, RSN is significantly stronger than WEP and WPA. However, it will run very poorly on legacy devices. Only the latest devices have the hardware required to accelerate the algorithms in clients and access points, providing the performance expected of today's WLAN products. WPA will improve security of legacy devices to a minimally acceptable level, but RSN is the future of over-the-air security for 802.11.

### *3.4.6 Advanced Encryption Standard (AES)*

AES is gaining acceptance as an appropriate replacement for the RC4 algorithm used in WEP. It uses the “Rijindale” algorithm in 128-bit, 192-bit and 256-bit key lengths. AES is considered to be un-crackable by most cryptographers. As part of the effort to improve the 802.11 standard, the 802.11i working committee is considering the use of AES in WEPv2. It will be implemented in firmware and software by vendors. AP firmware and client station firmware (the PCMCIA radio cards) will have to be upgraded to support AES. Client station software (drivers and client utilities) will support configuring AES with secret keys.

AES is a block cipher that can be used in different modes of operation. In 802.11i, two modes have been discussed: Offset Codebook (OCB) mode and Counter mode with CBC MAC (CCM). These two modes use AES differently to provide encryption and message integrity. OCB is a mode that provides both encryption and integrity in one run. CCM uses the Counter mode for encryption and CBC MAC for integrity.

### *3.4.7 Wireless Robust Authenticated Protocol (WRAP)*

WRAP is an encryption protocol like WEP and TKIP in the 802.11i standard and based upon the OCB mode of AES. WRAP protocol is removed from the last

specification of 802.11i. The AES implementation requires hardware support and the majority of legacy 802.11b products would not be able to run WRAP.

### *3.4.8 The CTR with CBC-MAC Protocol (CCMP)*

CCMP protocol is based on the AES encryption algorithm using the Counter Mode with CBC-MAC (CCM) mode of operation. The CCM mode combines Counter (CTR) mode for confidentiality and Cipher Block Chaining Message Authentication Code (CBC-MAC) for authentication and integrity. These modes provide good security and performance in either hardware or software. But legacy wireless equipment does not have the necessary hardware to support the CCMP protocol.

### *3.4.9 VPN and IPSec*

VPN technology provides the means to securely transmit data between two network devices. This technology has been used successfully in wired networks especially when using Internet as a physical medium. This success of VPN in wired networks and the security limitations of wireless networks have prompted developers and administrators to deploy VPN to secure WLAN connections. There are still lots of appliances and applications supporting VPNs in order to connect large number of remote sites or wireless clients in a WLAN environment. VPN works on top of the IP protocol. It provides three levels of security (Barken, L., 2003):

*Authentication and Authorization:* A VPN server should authorize every user who is logged on at a particular wireless station trying to connect to the WLAN using a VPN client. Thus authentication is user based instead of machine based.

*Confidentiality:* To provide confidentiality at the network layer, there is only one standard, IPSec, which is very complex. The complexity of IPSec contributes to a relatively high management overhead, at least at the beginning of deployment. IPSec solutions require the installation of client software on wireless stations to protect

outbound traffic. Perhaps the most frustrating attribute of IPSec is the difficulty in configuring two different systems to be interoperable.

### *3.4.10 Secure Socket Layer (SSL)*

SSL works by using a private key to encrypt data that's transferred over the SSL connection. It is a protocol developed by Netscape for transmitting private documents via the Internet. Both "Netscape Navigator" and "Internet Explorer" support SSL, and many WEB sites use the protocol to obtain confidential user information. By convention, URLs that require an SSL connection start with "*https:"* instead of "*http:"*

The industry-standard SOCKSv5, in conjunction with enterprise SSL, is currently one of the best available technologies for providing very granular access control. Enterprise SSL, a standard used for authentication and encryption, now extends across all IP applications, not just http-based, so that it can be used to strongly authenticate users and encrypt traffic in even the most demanding extranet environment.

### *3.4.11 Secure Shell (SSH)*

SSH is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over unsecure channels.

SSH is a well-known de facto standard for remote access and file transfer, as an easy to use alternative option to IPSec based security solution. "SSH Sentinel" provides smooth integration with the corporate resources via the Internet regardless of the type of connection, providing remote access and enabling file transfer, e-mail, Web browsing, messaging, and IP telephony.

### *3.4.12 Lightweight Extensible Authentication Protocol (LEAP)*

LEAP is a proprietary protocol which was developed by Cisco. It is an extensible authentication protocol that provides stronger authentication for newer 802.11 WLANs that support 802.1x port access control.

### *3.4.13 Protected Extensible Authentication Protocol (PEAP)*

PEAP is a proprietary protocol which was created by Microsoft, Cisco and RSA Security. It is an EAP type that addresses this security issue by first creating a secure channel that is both encrypted and integrity-protected with Transport Level Security (TLS). Then, a new EAP negotiation with another EAP type occurs, authenticating the network access attempt of the client. Password-based authentication protocols that are normally susceptible to an offline dictionary attack, can be used for authentication in wireless environments, because the TLS channel protects EAP negotiation and authentication for the network access attempt (S*ecuring Wireless LANs with PEAP and Passwords*, 2004).

### *3.4.14 Cisco Key Integrity Protocol (CKIP)*

CKIP is Cisco's version of TKIP, compatible with Cisco Aironet products. It adds security, performance, and manageability benefits to a wireless LAN network consisting of Cisco Aironet infrastructure and compatible third-party clients.

# CHAPTER FOUR
# THE PROBLEM CONSIDERED

## 4.1 Introduction

Many people entering the industry need to devote time to learn about it. It is important that the right tools and mechanisms are adopted from the start to ensure a well-managed approach to deployment. As the number of wireless users begins to grow, and Wi-Fi is used for high-speed and mission critical applications, the centralized management of the WLAN becomes important to provide network administrators with the ability to discover, manage, and upgrade access points across the network (Deploying 802.11 Wireless LANs, n.d).

It is really an important question how to deploy license-free wireless networks. Using free resources responsibly has never been easy. Anybody who is ready to deploy needs to cooperate and coordinate each detail. After weighing the pros and cons of the new deployment, it can be decided to implement a wireless LAN for the organization. One consideration in choosing the right wireless technology and topology is how well it will scale to meet your future needs.

## 4.2 Options For WLAN Standards

Most wireless networks today use one of the three variations of Wi-Fi technology:

-802.11b
-802.11a
-802.11g

It should be noted that the speeds given in Table 2.2 are stated maximum throughput. In practice, transfer rates will probably be lower than these. But, it should be kept in mind that even the slowest rate (about 5 Mbps effective throughput on most 802.11b networks) is still faster than the typical Internet connection.

There are other wireless networking technologies, such as Bluetooth and WiMAX (being developed as a long-distance wireless solution to connect computers over distances greater than the scope or the typical WLAN), not to mention satellite-based networking. This thesis will concentrate on the 802.11 variants that are commonly used to give wireless connectivity to a local network.

Several factors affect WLAN design. Some important variables such as, wireless network structure, wireless standards, number of potential users and their custom patterns, building layouts, security policies, product capabilities, ease of use, support and management, performance and future technologies in order to integrate with different networks need to be considered (Gust, M.S., 2002).

There are extensions that address weaknesses or provide additional functionality to the current Wi-Fi standards (Deploying 802.11 Wireless LANs, n.d). These are 802.11d, e, f, h, i, and j:

-802.11d addresses regulatory considerations in countries that do not have rules in place for the operation of 802.11 LANs. It ensures interoperability of WLANs in those countries.

-802.11e defines quality of service (QoS) levels for applications such as voice and video. 802.11 access points should be upgradeable via new firmware in the future.

-802.11f is the Inter Access Point Protocol (IAPP). It improves the handover mechanism in 802.11 between access points and switched segments as users roam between them.

-802.11h adds better control over transmission power and radio channel selection to 802.11a.

-802.11i provides enhanced security. It includes the use of 802.1x authentication protocol, an improved key distribution framework and stronger encryption via AES (Advanced Encryption Standard).

-802.11j addresses adding channel 4.9 GHz to 5GHz for 802.11a.

## 4.3 Main Concerns

It should be considered the scalability factors for each of the available technologies before plunging into wireless, or upgrading the existing 802.11b network. There is no “one size fits all” solution; the best choice for an organization depends in compatibility, distance range, and reliability. Most organizations will probably opt for the 802.11b/g combination because of the ease of transition, but those who use wireless communications for mission critical tasks and who need more security may find 802.11a to be a better option.

### *4.3.1 Speed*

Speed and distance can be important factors in scalability of a WLAN. As an organization grows, more users will be added. In addition, more bandwidth will be needed for the transfer of larger files and for higher bandwidth technologies such as streaming audio/video, real-time conferencing, etc. That means the more bandwidth, the better.

802.11a and 802.11g provide more scalability in this regard than 802.11b. With 802.11a, channels can be combined to get higher throughput.

### *4.3.2 Distance and Coverage*

Distance range can also be a factor in the scalability of a WLAN. As an office expands physically, more access points to reach the new areas have to be deployed. Access point devices typically have coverage areas of up to 100 meters. This

coverage area is called a cell or range. Users move freely within the cell with their laptop or other network device. Access point cells can be linked together to allow users to even “roam” within a building or between buildings (Phifer, L., 2003).

The maximum data rate is only available within a limited distance from an access point. Typically, this is 30m for 802.11b and 802.11g and 10m for 802.11a. If a client moves farther away, data speed is reduced. For example, an 802.11b client’s performance will diminish from 5.5 Mbps to 2 Mbps and finally to 1 Mbps as a user moves away from an access point. Therefore, it is important that access points are not placed too far apart.

Attenuation due to obstacles such as interior walls can reduce coverage as well. This is more of a problem for 802.11a, which is inherently less able to penetrate such obstacles. For larger sites, or buildings with solid interior walls, and RF site survey is a valuable tool in coverage planning (Cohen, A., & O’hara, B., 2003). Coverage planning is referred to as a site survey. Network managers gather data and make specific recommendations as to the types of access points, antennas, and other equipment to be installed and the specific locations for these installations.

Omni-directional design gives an increased wireless signal range in all directions (Figure 4.1). It also avoids the cost of adding additional access points. However, the directional design offers dramatically increased wireless signal coverage in a specific direction allowing for improved data throughput at further distances. One common error is to use omni directional antennas in two cells a short distance away from each other.

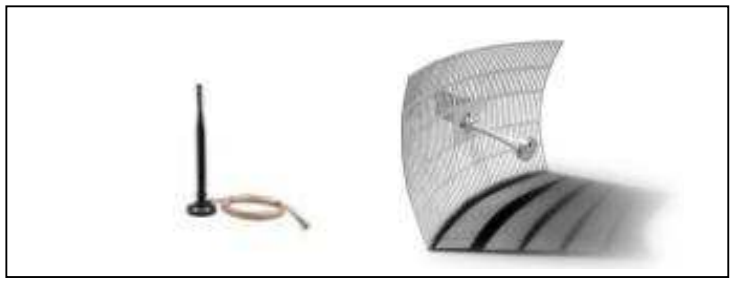

Figure 4.1 Omni-directional and Directional Antenna Design

### *4.3.3 Compatibility*

Another factor that affects scalability is compatibility, and this is a two-pronged consideration:

-Compatibility of wireless technologies with one another,

-Compatibility with wireless devices, especially the network adapters built into many of today's notebook computers.

A big advantage of 802.11g over a is its backward compatibility with 802.11b. It can be started with an inexpensive 802.11b wireless AP and then be replaced with an AP that supports both b and g. Computers that have 802.11b network adapters will still work, but at the lower 802.11b speeds. NICs can be replaced for making a smooth transition. If it is decided to switch into 802.11a, everything will have to be replaced immediately because it is not backwardly compatible with the former 802.11b equipment.

Another problem with 802.11a is that the built-in wireless equipment in notebooks is almost of the more common 802.11b or “g” varieties. This will cause a problem for the 802.11a infrastructure, because it is necessary to turn the built-in wireless cards off and add 802.11a NICs.

Finally, employees who connect to a wireless network may also want to connect to other wireless networks at their homes or at public access points ("hot spots") in hotels, airports and restaurants. Most home and public wireless networks use 802.11b technology, so they'll need to swap out two different NICs (or use built-in wireless for home/public networks and a separate NIC for the corporate wireless network).

### *4.3.4 Channels*

Channels are important, because they affect the overall capacity of the WLAN. A channel represents a narrow band of radio frequency. Since radio frequency

modulates within a band of frequencies, there is limited amount of bandwidth within any given range to carry data. It is important that the frequencies do not overlap or else the throughput would be significantly lowered as the network sorts and reassembles the data packets sent over the air.

It should be ensured that the selected channel is compatible with the channel ranges supported by the wireless clients. To ease administrative burden, it is necessary to look for an access point that can automatically scan the spectrum of all available regulatory channels, and select the one with the least interference. The best channel is the channel where no other wireless devices are causing interference on the RF.

Clever architectures to suit the range and density requirements can be constructed using the non-overlapping channels of 802.11a and 802.11b. For instance, “cellular architectures” can be deployed by mixing the three non-overlapping channels (channels 1, 6, and 11) of the 802.11b standard, while minimizing the risk of inter-access point interference.

Knowing that the 802.11a specification operates at radio frequencies between 5.15 and 5.875 GHz, and the 802.11b and 802.11g specification operates at radio frequencies in the 2.4 to 2.497 GHz range, it can be seen that the 802.11a has a wider frequency band, allowing more channels and more overall throughput. The wider frequency band allows 802.11a to support up to eight non-overlapping channels and 802.11b/g to support up to three non-overlapping channels.

Each channel will carry a maximum throughput for its standard. Therefore, the 802.11b and 802.11g standards have a maximum of three non-overlapping channels carrying 11 Mbps throughput each (33 Mbps total) and 54 Mbps (162 Mbps total) throughput. The 802.11a standard has a maximum of eight non-overlapping channels carrying 54 Mbps throughput each, or 432 Mbps total throughput.

### *4.3.5 Capacity*

Capacity planning is an absolute with Ethernet,: the number of users connected to a single hub is the same as the number of users in the collision domain. With Wi-Fi, on the other hand, the number of users can vary greatly as they enter and exit the coverage area. Additionally, with transmission over radio waves, throughputs present themselves in the coverage area.

The goal of capacity planning is to provide users with what they need, the goal of coverage planning is to provide them with what they need where they need it. The central question that needs to be answered is: “How much throughput should be provided to each user of the WLAN, on average?”

### *4.3.6 Reliability*

Up to this point, it may seem that 802.11b/g is the clear choice, but there is one more important factor to consider. In order to scale to meet the networking needs, WLAN must be reliable. An unreliable technology isn’t scalable because it doesn’t make sense to expand its deployment if it isn’t counted on to work properly.

This is where 802.11a has the home-court advantage. Because of its incompatibility since it operates on a different frequency from other popular wireless networking and consumer communications technologies, it’s far less prone to interference that can bring the network down or disrupt transmissions.

Another aspect of reliability is security, and 802.11a enjoys a form of “security through obscurity”. Simply because it’s not as widely deployed and the equipment costs more, fewer hackers target networks based on 802.11a.

## 4.4 Network Management

Network management encompasses a number of key functions: monitoring the network's activity; dynamically evaluating its availability; measuring its performance; and logging its errors. These functions are more important, not less, where the wireless portions of the network are concerned. Since the wireless zones are more portable, more variable in usage, and subject to greater interference than the conventional ones, performance tracking and error logging are more important than ever if it is hoped to optimize the network's efficiency.

It's not just about efficiency, of course. By doing this sort of management, what happens at the access points can be monitored and network intrusion attempts can be spotted at. So, implementing network management of the wireless network zones is a wise move.

### *4.4.1 Network Audit*

Wireless components in a LAN do not affect the ability to audit the network as a whole. There is nothing essential to wireless devices or access points. One can continue to audit the network as it is normally done.

An additional consideration in the audit process, where wireless access points are concerned, is that the access points themselves can generate logs. These logs record the activity of stations connecting to them to gain network access. These logs need to be integrated into the audit process and regularly reviewed.

### *4.4.2 Control Rogue APs*

Rogue access points are one of the biggest headaches in wireless network security. Rogue access points are those installed without the IT departments knowledge and are generally not configured with any security settings, which leaves an open door for unauthorized access.

That's a great deal of vulnerability, and it tells that rogue APs alone are justification for implementing stringent network management procedures. APs placed strategically throughout the network environment that can be managed from a central, remote location should be a consideration when deploying a WLAN. With SNMP-based network management software in place, the network can rapidly identify any rogue APs that employees have deployed.

Another way to detect rogue APs is use a WLAN scanner (the way hackers do it). A laptop with a wireless network card and WLAN-detection software such as “NetStumbler, Air Magnet, or Wave Runner” can sniff out all the APs.

### *4.4.3 Test Your Fences*

The best way to feel good about the company’s wireless perimeter security is to test it personally. Anyone with a laptop, a wireless network card, and “NetStumbler” can cruise the streets around the HQ and map the network. WLAN intruders use these tools and various nefarious means of entry to get into the network.

## 4.5 Effectiveness of Basic WLAN Features

With any network technology, standardization is key to widespread adoption. More specifically a standardized protocol is required that governs how WLAN system devices communicate with access points to ensure interoperability and to avoid having to buy from only one vendor.

WLANs also create some extra administrative and security headaches. Centralized security and management of wireless LANs is a rapidly growing trend in which a WLAN device such as a switch, appliance, or router is used to create and enforce policies streamlined.

### *4.5.1 Network Performance Requirements*

Depending on the applications used on the wireless network, different requirements are imposed. One of the most important items, and the one that is least under the control of the network architect, is the characteristics of the application. Most applications can be run over TCP/IP, but they may require widely varying throughput, delay, or timing characteristics. More importantly, though, is how an application reacts to network address translation (NAT).

### *4.5.2 Mobility*

Wireless devices (with the exception of laptops using wireless cards) possess limited computer-processing power. Since databases consume a lot of memory, companies that must have wireless databases should load only essential subsets of data that could fit on smaller devices.

The most prominent characteristic of the wireless mobile networks that differentiates them from fixed wireline networks is the requirement to share a limited spectral bandwidth. They also cope with the contention and mutual channel interference resulting from a large number of randomly located mobile users. Furthermore, the wireless communication links themselves can be described as time-varying frequency-selective fading multipath channels. The topology, link performance and quality of service (QoS) delivered to user applications in this communications environment is characterized as highly time-varying.

Another differentiating characteristic, especially in data networks is that the user mobility imposes new requirements on the architecture of these networks. Existing data networks, which were designed and implemented, must be extended to allow users to attach to different parts of the network and receive services as they were attached to a fixed home location. To judge from the lack of commercial offerings in wireless mobile data networking, supporting this type of operation in today’s data

networks is a much greater challenge than simply providing roaming telephone service.

### *4.5.3 Roaming*

One of the most valuable capabilities is support for roaming and session persistence. Some organizations implement WLANs using a flat address space and enforce policy where wireless and wired networks meet. However, most enterprises want the flexibility to install wireless access points on multiple subnets and when devices roam between subnets, problems can occur.

Roaming is a critical component of the mobility equation. Wireless clients must be able to roam among all access points within the same or different subnets. Routing mechanism rely on the assumption that each network node will always have the same point of attachment to the network, and each node's IP address identifies the network link where it is connected. If a mobile device is disconnected from the current network and reconnected through a different network, the device should be configured with a new IP address, the appropriate net mask, and default gateway.

### *4.5.4 Interference*

An interfering signal causes an energy jump in radio transmission and may start abruptly in the middle of a transmission causing a collision. The presence of unavoidable interfering RF signals disturbs IEEE 802.11 operation. When the power of the interferer is significant, it may cause the client stations to become inactive for indefinite periods until the interference disappears.

### *4.5.5 Discovery and Configuration*

Administrators need to have tools that allow them to discover various wireless devices within the network segment, configure parameters, run diagnostics, monitor performance, view device properties, and select a device for individual configuration.

They protect each network infrastructure access point by setting necessary parameters to control access to the configuration settings.

To ease administrative burden for larger networks, capabilities such as “save and load facility” are useful because they allow to configure one device and propagate the same configuration to similar devices on the network.

## 4.6 Main Security Problems

Security is also a primary concern. The access to the network and data protection are two elements of WLAN security. They are known respectively as authentication and encryption. Security breaches commonly come from rogue APs which are set up by employees without the knowledge of the network administrator and installed with the security features turned off. The individual PC can also be a security risk if it connects to a network in ad hoc mode or operates in peer-to-peer fashion. To protect a wireless LAN network, both security elements need to be addressed (Ryan,V., 2003).

### *4.6.1 Challenges to Securing Wireless Networks*

In modern network technologies, physical boundaries between public and private networks no longer exist. Wireless network is an example and the security implications are apparent. Whether a user has the necessary permissions to access a wireless system can no longer be assumed on the physical location. First, wireless networks do not have firm physical boundaries, and frames are transmitted throughout a general area. Attackers can passively listen for frames and analyze data.

Second, data is broadcast using radio frequencies, which can travel beyond the control of an organization. To defeat attacks against secrecy, network security engineers must employ cryptographic protocols to ensure the confidentiality of data as it travels across the wireless medium.

Third, wireless hosts may compromise integrity. Quick wireless LAN deployments are often connected directly to a supposedly secure internal network, allowing attackers to bypass the firewall. In many institutions, internal stations are afforded higher levels of access privileges. Attacks against integrity may frequently be defeated by strong access control (Piscitello, D.M., 2002).

### *4.6.2 Access Control and Authentication*

Connection to wireless networks is designed to be easy. The ease of connection is one of the major advantages to many newer wireless technologies. Strong access control should be applied to protect networks against the threat of unauthorized access. APs are like open network drops in the area.

802.11 networks can benefit from access control at two points: Before associating with an access point, wireless stations must first authenticate. At present, this process is either nonexistent or based on WEP. After association with the access point, the wireless station is attached to the wireless network. However, strong authentication can be applied to any wireless stations to ensure that only authorized users are connecting to protected resources.

One approach is to allow only a specified set of wireless LAN interface MAC addresses to connect to access points. A second approach is to allow connections from stations that possess a valid WEP key. Stations that pass the WEP challenge are associated, and stations that fail are not. In some products, these methods may be combined. However, both are easily defeated.

### *4.6.3 Confidentiality*

Confidentiality is the second major goal in wireless LAN deployments. Traffic is left unprotected by default, and this is an inappropriate security posture for most organizations. Users can choose among four options:

#### *4.6.3.1 Using WEP*

The choice really comes down to whether WEP is good enough. WEP is not strong encryption, and it should be assumed that a sufficiently motivated attacker could easily capture traffic, recover the WEP key, and decrypt the data. In most WEP deployments, keys are distributed to every authorized station. When all users have access to the key, the data is protected from outsiders only. WEP does not protect an authorized user with the key from recovering the data transmitted by another authorized user. If users need to be protected from each other, which is a common requirement in many computing environments, then additional security precautions are required.

#### *4.6.3.2 Using WPA*

Every device on a wireless network must be upgraded to WPA in order for the new standard to take effect. If some devices still use WEP, the entire network will fall back to the older, weaker security algorithm. This could be a problem in configurations of Wi-Fi products assembled from multiple vendors, especially if vendors are slow to offer the software upgrade. WPA employs a central server to authenticate each individual seeking to join a network.

#### *4.6.3.3 Using a Proven Cryptographic Product Based On Open Protocols*

Choosing a cryptographic protocol or product is subject to a few basic ground rules. If a protocol or algorithm has withstood extensive public analysis, it is probably better than something just invented.

#### *4.6.3.4 Using a Proprietary Protocol*

This method locks the users into a single vendor and leaves them at their mercy for upgrades and bug fixes. Proprietary cryptographic protocols also have a poor track record at ensuring security.

### *4.6.4 Mobile Device Security*

Wireless technologies generally come with some embedded security features. But many of the features are disabled by default. As many newer technologies, the security features available may not be as robust as necessary. Because the security features provided in some wireless products may be weak to attain the highest levels of integrity, authentication, and confidentiality. Agencies should carefully consider the deployment of robust, proven, and well-developed and implemented cryptography.

Mobile devices now offer features and functionality approaching those offered by desktop and laptop computers. The role of mobile devices in the enterprise is expanding quickly, ranging from use by individual employees to full enterprise deployments. Price, size and end-user attention are the main characteristics of these mobile devices that make them inherently vulnerable to a wide range of security threats. In addition to the databases of business contacts and appointments that commonly exist on both personally owned and enterprise-deployed mobile devices, a wide range of new functionality, including email attachment viewing, office document editing, and file storage, makes it quite possible that these devices may hold more sensitive data within their memory. Clearly, the potential for the storage of sensitive data on mobile devices is high and growing.

#### *4.6.4.1 Loss or Theft*

Lost or stolen mobile devices represent the most common threat scenario. Placed for a moment on a table, dropped from a pocket, or left in a vehicle, mobile phones or handheld devices can be easily misplaced by employees. Once in the hands of an unauthorized user, most mobile devices have only limited basic security solutions to protect stored information. Furthermore, many of these basic solutions require end-user commitment to their use and can be easily disabled if the end user considers them unnecessary.

If employees do not protect their mobile devices with a password, then data stored on these devices becomes immediately available to the unauthorized user. Even if a password is used, if the data itself is unencrypted, a dogged intruder with the correct tools can lift that data directly from device memory. As a result, fraud and theft of data as well as corporate espionage become easy tasks.

#### *4.6.4.2 Interception and Intrusion*

The growing methods of data transmission represent many virtual conduits through which sensitive corporate data may flow to and from a mobile device. Although solutions exist to ensure the security of these conduits, insecure transmission of information is quite common. Furthermore, omnipresent wireless connectivity provides fertile ground for remote intrusion into devices themselves.

#### *4.6.4.3 Malicious Code*

Because mobile devices offer capable platforms and deep applications capability, they are easy targets for viruses, Trojan horses, and other types of malicious code. These codes can not only corrupt and destroy local data on the mobile device, but they can also spread to the host enterprise network via computer synchronization or send sensitive information wirelessly.

### *4.6.5 Security Management*

Administrators should be able to define user profiles “on-the-fly” and manage them quickly and consistently across multiple platforms. They should be able to back-end to standard databases in order to prevent replication of user groups and it should be easy to enforce security policies, centrally, remotely, or through a distributed system. Traffic can be proxied through one or more central servers, where security policies and user profiles are managed and auditing data is collected.

Client software should not require any training for the end user and should run transparently on the desktop without interfering with any applications, drivers. It should also work on all key platforms and be easy for an administrator to configure and distribute centrally. It is simply not a practical option if someone has to visit every desktop to install or configure the client software.

### 4.7 Key Problems

Some of the important problems that will be addressed by this research are:

1.What are the criteria to build a wireless network in a specific time and place?

2. How can Wi-Fi best be integrated into the wired environment?

3. Where does Wi-Fi add a vital mobility element to a network?

4. How much time is needed to configure the wireless LAN?

5. How flexible is the configuration of the network?

6. Can a user roam freely on the network?

7. What restrictions on roaming are there?

8. Does the infrastructure of the network support required security policies?

9. What are the problems before setting up a WLAN during the field exercises of the Army?

# CHAPTER FIVE
# A NEW APPROACH TO WLAN

## 5.1 Introduction

There is an increasing need in the military for high-rate reliable wireless communications in a limited and crowded spectrum. Wired and wireless networks have to be treated as one entity. This is a good way to keep WLANs under control and safe from security breaches.

This chapter gives a typical overview of basic security issues that will be followed in the planning and implementing phases of critical WLAN systems especially in the area of potential Military applications. First, it analyzes the implications of the network managers or CIS planners before setting up an official independent WLAN or as an extension of the currently used wired networks. Before the deployment of a new wireless network, a detailed project plan should be taken into consideration and the pros and cons of the new architecture should be figured out. After providing background information on Army requirements and constraints about WLANs, and discussing the implementation issues, a template of wireless network model is validated for the required critical values written in the official directives. Next, a reasonable wireless policy that can be followed up by the Army and will help and lead network managers to a proper way to follow up the future probable WLAN practices, is presented for future use.

## 5.2 Wireless LAN Usage Concept

Wireless LAN has become increasingly popular in recent years for its advantages of simplicity and mobility. However, lots of WLAN deployments are held back in the Army and the other main governmental organizations, because of security concerns. The reason is that the Army has strict security rules in this type of networking. This is mainly due to the risks, threats, and vulnerabilities associated with the wireless communications.

Since the Army units are mainly mobile and deployable with the tactical and operational purposes, they require both classified and unclassified data transfers over the wireless communications links. Therefore, integrating WLANs to existing official wired network infrastructure could be beneficial to the tactical military operations. Because, it will reduce the setup time and costs associated with laying wires. It also decreases the manpower needs required to install, operate, and maintain the local area network (LAN). With technological advances in WLAN standards and security, the existing threats and vulnerabilities can be mitigated to an acceptable level in the future.

Army and the Civilian Organizations have begun establishment of the first WLAN use. WLANs are being used primarily for public Internet access and as an extension of the current wired networks.

Building a wireless project plan that will align with the organization strategy is essential to ensuring success. For many network engineers and CIS planners, the amount of time it takes to develop such a plan, and the complex process required to complete it, makes this planning a frightening task.

### 5.3 Army Requirements

Introducing wireless technologies would provide the possibility of much more rapid setup of communications during tactical or operational deployment or re-deployment. Additionally, the flexibility, mobility, and performance characteristics offer a lot of advantages. Security for voice and data transfers is of utmost concern during WLAN deployment. The requirements for establishing a WLAN would be particular to the military units or organizations to deploy in the area of a few hundred meters in diameter, not for covering longer distances.

Some of the basic step-by-step process of designing and installing a successful WLAN should be examined. The first set of steps is gathering and analyzing

requirements. “Make sure that all of the real-life usage requirements are well understood for the users’ performance expectations.”

### *5.3.1 Quick Set-up and Mobility*

Army typically deploys to the different locations for exercises, reconnaissance and a variety of alert status, where some of these regions do not have a regular commercial communications infrastructure. Information Systems personnel would like to have the capability to set up the Headquarters’ (HO) communications requirements in the new location with a minimum loss of time and service.

In a new deployment, an initial entry patrol is used to physically secure the area. Their only need is simple voice capability. Once the main unit gradually deploy into the region, communications capability will focus from force protection to administrative tasks for the HQ. This will increase the number of users and data circuits. Communications Information Systems (CIS) units have to be ready to provide voice and data in this phase, according to the written Standard Operating Procedures (SOP) of the HQ. WLANs would be extremely useful in this type of deployment, with their flexibility and easier planning considerations.

As the units grow, the Tactical Operations Center (TOC) tends to be a very fluid and dynamic workplace in the field. Many new users are added and shifted as new specialties (e.g. logistics, medical, intelligence) arrive at the area. Once the situation matures and the size of the unit becomes more stable, the WLAN would still benefit the CIS planner. Because CIS planner will have a a great deal of flexibility, save manpower hours of running wires and cables, and reduce cost sustaining and supporting the network (Powers, J., & Hynes, K., 2005).

### *5.3.2 Cost*

When the cabling is expensive or physically impossible to run due to the geographical structure of the region, WLANs appear to be an alternative. By using

fiber optic cables, the communications range for 100 Mbps bandwidth can be increased to a few kilometers more. However, the installation difficulty and cost will be very high. Therefore, fiber solutions are not reasonable if this rate is not really required. Finally, WLAN use in long distances for considerable amount of bandwidth performances is more than enough.

One of the WLAN benefits is that CIS planners can use Commercial Off The Shelf (COTS) technology instead of developing the necessary devices in-house. At first glance, this would not seem to be a secure solution for the Army, instead of developing their specific WLAN technology. Army is used to develop their own technology and automation products in order to be less vulnerable to known malicious attacks. However, this is unfeasible for the Army due to the budget constraints and compatibility problems. Until a military product is being improved, it has already been passed by the civilian sector and began to be used.

By using COTS products, Army increases the security state by having more up to date products instead of developing its own devices (Powers, J., & Hynes, K., 2005). This will shorten the development life cycle of the products and allow Army and Defense Industry to focus more on their core competencies.

### *5.3.3 Longer Range*

WLANs should provide the necessary bandwidth that the users require for their applications and a large coverage for the whole area. Current WLAN technologies offer 50-200 m. ranges with their standard and mandatory power output limits. Increasing the cell sizes and range requires different technologies and brings additional device cost for each cell. In order to be sure that the right selections of higher frequencies are made, it has to be assumed which technologies offering higher bandwidths can be applied.

Assessing environmental radio coverage including the selection of trial component, installation areas where signal loss is avoided or minimized. The optimal positioning of access points and antennas is also determined.

## 5.4 Army Constraints

If military WLAN requirements are translated into technical specifications, it will discovered that the wireless environment is full of with constraints and incompatibilities. There are constraints and restrictions related to physical infrastructure and the environment. It may be discovered that the original solution cannot be deployed as envisioned as limitations in military areas. Some wireless constraints are temporary. Over time, the rapid evolution of wireless capabilities will reduce constraints in areas such as, security, bandwidth, coverage, and support tools.

### *5.4.1 Security*

The security vulnerabilities of wireless LANs aforementioned in chapter 3 have already been discussed since 1999 and taken into consideration to be developed until now. WLANs should meet the necessary security criteria and standards as written in the official directives used by the Army. Even though they aren't presented in detail, some of the main security issues which are unique to wireless networking, is explained in the following paragraphs and give an idea how to design and build a secure network (Potter, B., & Fleck, B., 2002).

#### *5.4.1.1 Identification and Authentication*

Preventing unauthorized access to sensitive mission-critical wireless networks is a key requirement. Maintaining 100% network availability and confidentiality for sensitive information processed, transmitted, and stored in a WLAN is extremely critical. According to the Army Communications and Information Systems Security Directives, cryptographic and encryption techniques should be determined by National Agencies, because they provide the most efficient and recommended

methods to safeguard the information on wired and wireless LANs. In an International Military Environment, NATO standards discuss the applicability of wireless technologies ranging from “Bluetooth” and WLANs through Line-of-Sight Radio Relay for different tactical in different scenarios. New wireless standards like 802.11i use AES integrated with 802.11x authentication standard. Therefore, such a robust security mechanism allows a capability to achieve quick and cost-effective establishment and deployment of WLAN infrastructure in the HQ or related locations (NC3A Technical Note, 2003).

802.1x will provide more authentication and access control for APs using extensible authentication protocol (EAP), which is a set of messages for authentication negotiation and authentication transport method between the clients and the server Using EAP, 802.1x will allow for interoperability with multiple authentication technologies like RADIUS, token cards, KERBEROS, and PKI. However, 802.1x requires additional servers like RADIUS that is not ideal for a tactical environment, and still has the suitable lack of industry testing (Nortel Networks, 2004).

*5.4.1.2 Encryption*

WLAN using “SECRET” level of classified information must not be operated without the encryption. Army and the critical organizations require that a national encryption algorithm must be provided before they use the SECRET information thorough the wireless links.

802.11i improves on WEP by using completely new encryption algorithms and key-derivation techniques. This wireless security standard, finalized in June 2004, makes it possible to safeguard over-the-air communications at Layer 2. 802.11i also referred to as Robust Security Network (RSN) that is designed to address all the security issues associated with 802.11a, 802.11b, and WEP shared key encryption. This standard includes two parts: the AES for encrypting WLAN traffic and IEEE 802.1x Port-based network authentication standard for WLAN user authentication

and key management (Atheros Communications, n.d). AES can be adopted for wireless network encryption. However, the advanced 128-bit, 192-bit, or 256-bit encryption algorithm requires higher processing power to encrypt and decrypt. Nevertheless, the latest wireless standard 802.11g implemented with IEEE 802.11i using AES encryption will satisfy wireless encryption requirements.

If the original DES (Data Encryption Standard) algorithm is tested for the robustness of the algorithm which is nearly 30 years old, it is a testament to IBM and the U.S National Security Agency that there are still no practical cryptanalysis techniques to break DES. The fact that DES can be brute-forced is irrelevant because the short key length of 56 bits can easily be tripled using 3DES, which makes more combinations. The official successor to 3DES is AES, which has key lengths between 128 bits to 256 bits and was fully examined by the security communities. Most VPN or encryption products rely on 3DES and AES and they currently have absolutely no need to change their encryption algorithm (Ou, G., 2005).

### *5.4.2 Design*

The geographical structure of the new command post and the distances between the fixed and mobile systems are very important together with the bandwidth requirement. Three types of system requirements are assessed; Type A is the office environment with a group of single users. Type B represents the infrastructure within the HQs and connects the offices to the core CIS switch. The last, Type C is a Short Range Line-of- Sight radio link to connect locations within the same geographical area.

The commercial WLAN standards for Type A requirements offer good support and can be found easily in the market. The security on these links is either nonexistent, or provided at Layer 3 (IP Sec) or higher. New access control protocols are being implemented commercially and increasing security in the sense of unintended intrusion logging, denial of service attacks.

A range of standards has been released recently for the Type B requirement, both by ETSI (European Telecommunications Standards Institute) and IEEE. However, there has been promoted compliant to these standards yet. Commercial proprietary solutions with very similar performance and architectures could be used for tests and trials. Experts expect that products will be certified compliant by the end of this year.

There has always been a wide range of available systems for the Type C requirement, mainly due to the similarity between the defined requirement and the structure of a network. In this segment, many proprietary solutions are available, but standardization can be a problem except for the management of the network (Ou, G., 2005).

There are limitations for different classification levels such as NU (NATO Unclassified) and NS (NATO Secret) that require different security domains. Even, in wired networks, these different domains should have the appropriate infrastructures. WLAN design presents the network managers and CIS planners some obstacles. A seamless and secure distribution of information has to be provided in spite of competing hardware, software and network problems.

In a WLAN environment, serving to the buildings or deployed elements beyond, the coverage is impractical. Therefore, network managers should think over the necessary range considerations in the area.

### *5.4.3 Interference*

Wireless networks require far more deployment planning because of the nature of the radio link. Every building has its own personality with respect to radio transmissions, and unexpected interference can pop up nearly everywhere. If two different WLAN systems using the same RF bands are located in the same or nearby areas, the interference occurs. Interference is caused either by an access point or a WLAN client Ethernet card. Some materials and surfaces are prone to reflection and cause RF signals to bounce off materials and return. These signals create a multi path

phase cancellation of the original signal. Reflective materials include metal, lead-based curtains and glass with heavy lead content (Network Project, 2005).

Other WLAN networks can also cause interference. Older cordless phones cause the same problem by occupying wireless channels. “Bluetooth” running at 2.4 GHz frequency band has an important degradation of access point performance when working close to it. Microwaves and fluorescent lights have similar diverse effects.

### *5.4.4 Developments and Technology*

The technologies around us in our daily life are unavailable to our current military use. The level of security required to run the proper Information Systems based on the official directives in a deployment, can make the application of commercial solutions less available in the military side. National Defense Agencies work heavily for the development of national wireless network systems containing stations, antennas, NICs, and APs as well as the national crypto mechanisms.

The wireless protocols and devices have to be determined in the phase of technological review before setting up a WLAN. Plan should include the short and long term evaluations, replacement of current technologies and future plans for WLAN.

802.11b WLAN deployments tended to be relatively small but large enough for different levels of HQs or a medium sized corporate networking needs. However, enterprise users run into bandwidth problems due to capacity issues or radio channel conflicts. Users share a data rate of 11Mbps or 54Mbps with 802.11 standards depending on distance.

Network managers want to extend their WLAN’s ability by adding VoIP on their applications for their users. WLAN infrastructures are designed with either in one standard or in all three current WLAN standards. 802.11b/g/a WLAN based products are recently in the market. 802.11a/g standard offering a seamless 54Mbps provides

streaming video. One major security concern with using 802.11g for military operations is the 2.4 GHz frequency which is a widely used ISM (Industrial, Scientific, and Medical) band. An unauthorized person can easily jam the wireless traffic or start a Denial-of Service (DoS) attack with a powerful transmitter. Army can decide to use another frequency allocated for the military use or a different modulation technique to withstand this risk.

Army does not specify a particular WLAN technology for the tactical purposes. The goal is to provide an important framework for the integration of existing and emerging WLAN technology. Security accreditation is based on the NATO standards and National Cryptology Agency parameters.

### 5.5 WLAN Standard

Army Commands apply some features of WLAN standards for the different level of Tactical Communications in the area. The mobility itself for the applications and projects is more important than the other useful features of Wireless Networks.

The standards appear to be able to provide comprehensive solutions to WLAN security issues today. Features of 802.11 WLAN standards including 802.11b, 802.11g, and 802.11a are listed in Table 5.1(Wei-Meng, L., 2003).

Table 5.1 Features of 802.11 family standards

| Name | Spectrum | Data Rate | Distance |
|---|---|---|---|
| 802.11b | 2.4 GHz | 11 Mbps | <100 m. |
| 802.11g | 2.4 GHz | 22/54 Mbps | <100 m. |
| 802.11a | 5 GHz | 54 Mbps | <50 m. |

802.11b is the standard widely used, deployed, and tested product at present. It is cheap and robust. In most cases, this will lead to choosing 802.11b-based networks. A 802.11b WLAN may be right if data rates up to 11 Mbps are sufficient. It has better range and wall penetration. If there is a requirement to expand an existing

802.11b WLAN and WLAN access for handheld PCs, 802.11b is more suitable. However, it will have a small number of users per access point

802.11g is still a work-in-progress standard while preserving the available features of 802.11b. An 802.11g WLAN may be right if it is needed to enhance throughput up to 54 Mbps and extend the existing 802.11b network. It will have the necessary bandwidth and its speed will handle large graphics, audio, data, and video files. Range and wall penetration advantage also work for 802.11g. It is ideal for meeting the required bandwidth and critical security features with the Orthogonal Frequency Division Multiplex (OFDM) modulation technique, in the tactical environments. It supports interoperability with PKI certificates and AES encryption requirements (Geier, J., 2003).

802.11a operates in a different frequency band and gives a higher speed and a shorter coverage distance. 802.11a will not be compatible with 802.11b and 802.11g. If you like leading-edge technology, you may want to consider 802.11a products. An 802.11a WLAN will be right for you if you need enhanced throughput up to 54 Mbps and need the bandwidth and speed to handle large graphics, audio, data, and video files. If it is required to avoid interference from other wireless devices, 802.11a has the advantage. If there is a need for more users, it is the only alternative.

With the improvements of 3G (Third Generation) GSM (Global System for Mobile Communications) systems today, wireless industry standards will move another platform for the different system architectures.

**5.6 Radio Frequency and Channels**

Electromagnetic spectrum is one of the natural resources of each sovereign nation. The employment of a WLAN requires the approval of host nation telecommunication authorities and complies with the frequency allocation tables. Next, it is important to consider the type of the communications network that will work best for the application. The major decision points are to choose the communications technique,

frequency, and standard. As shown in Table 5.2, the 802.11 standard has widespread frequency allocation support in the World.

Table 5.2: Channel Support

| Standard | Interface | Frequency | Number of Channels in the Approved Frequencies | |
|---|---|---|---|---|
| | | | Europe | US |
| 802.11b | CCK over DSSS | 2.4 GHz | 4 | 3 |
| 802.11g | CCK over OFDM | 2.4 GHz | 4 | 3 |
| 802.11a | OFDM | 5 GHz | 0 | 12 |

Following the NC3A Tactical WLAN ideas and proprietary solutions aimed at moving to a different frequency range can cause for similar implementations as the new standards.

Channels are important to understand because they affect the overall capacity of the WLAN. A channel represents a narrow band of radio frequency. WLAN utilizes non-overlapping RF channels, supporting a clean, interference-free signal for computing systems and mobile devices. Increasing the number of non-overlapping channels increases performance capacities. The IEEE 802.11b and 802.11g standards have three non-overlapping channels and provide ample support for users requiring Internet and e-mail functionality. The IEEE 802.11a standard, with eight non-overlapping channels, provides maximum bandwidth with capacity to transfer larger data and graphic bit-intensive files whether conferencing or working in a collaborative environment.

The number of radio frequency channels required by an organization is determined by assessing usage requirements. For example, a public hotspot such as a lobby can usually be well supported by the 802.11b standard for e-mail support or viewing of Web sites a conference room may be better served by the 802.11a standard for transfer and collaborative work with data files, and a home office might best suited by a 802.11g based network.

## 5.7 Architectural Topology

Figure 5.2 shows the topology between access points and wired backbone network. Main servers and APs are placed in a WLAN deployment roughly behind the backbone switch/hub as shown in this figure.

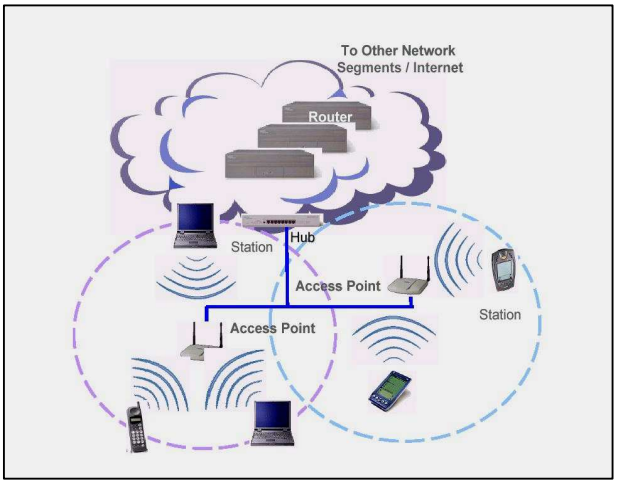


Figure 5.2 Standard WLAN deployment topology

### *5.7.1 Access Point*

The number of simultaneous users that an access point can support depends mostly on the amount of data traffic at the time. Bandwidth is shared among users on a WLAN as with wired network connections. In 802.11b, each hardware access point has up to 11 Mbps throughput and can support a large group of simultaneous users as effectively as Ethernet. The approximate numbers for different ratios of usage are:

-50 nominal users who are mostly idle and check an occasional text based e-mail,

-25 mainstream users who use a lot of e-mail and download or upload moderately sized files,

-10 to 20 power users who are constantly on the network and deal with large files.

More access points may be added to increase capacity, which gives users more opportunity to enter the network. Networks are optimized when the access points are set to different channels. For instance, a company may place three 802.11b access

points (with a range of up to 100 meters each) in three adjacent offices, with each unit set to a different channel. In theory, many users could then share up to 33 Mbps total capacity (although no single user would ever have throughput faster than 11 Mbps). In reality, clients associate with the access point with which they share the strongest signal, so the bandwidth may not be dispersed evenly among users.

Access points must be placed to proper locations to provide good coverage so that offered services, user needs and expected traffic load requirements are satisfactorily met. The estimation technique aims to guarantee service with good quality and offers capacity with a sufficient low congestion. A static network configuration is not adequate for WLANs because it does not take into account how expected behavior of the user. Users might cluster in allocation for sometime and then move to another location. In this case, access points must be properly configured in real-time to meet traffic demand.

Performance is improved by using an AP that provides additional network services such as, print server, DHCP, router, and switch.

### *5.7.2 Access Controller*

The use of access controller reduces the need for smart access points. An advantage of placing the access controllers is that the system is easier to support, primarily because fewer touch points are in the network. If all of the intelligence of the network is within the access points, support personnel must interface with many points when configuring, monitoring, and troubleshooting the network. An access controller enables the access points to have fewer functions, reducing the need to interface with the access points when performing support tasks.

Several wireless LAN vendors offer specialized "wireless access controller" devices, which typically combine packet filtering, authentication, authorization, and accounting services (AAA), and a DHCP server; many devices also include a DNS server and VPN termination. AAA features are typically provided by an interface to

an existing corporate infrastructure such as RADIUS, which frequently has already been configured for remote access purposes. Some products may also include dynamic DNS so that a domain name is assigned to a user, but the IP number can be assigned with DHCP.

### *5.7.3 Antenna*

MIMO (Multiple Input, Multiple Output) is a smart antenna technology for wireless communications, employing multiple antennas for reception and transmission at each end. Using digital signal processing to mitigate the impact of multipath effects, MIMO can significantly improve both throughput and the range of wireless communications. MIMO is expected to be a key component of IEEE 802.11n, the next generation of Wi-Fi. MIMO has started appearing in premium wireless products.

The same equipment used in wireless LANs can also be deployed in bridge mode to connect buildings in the same area. Changing the antenna from one that's omni directional to one that's directional does this. The idea in changing the antenna is to restrict the signal to just the area between the two buildings. There are several problems with this method. Antenna selection is also critical in determining exact positioning of access points. Different antenna designs produce different propagation characteristics.

## 5.8 Deployment

Wireless networks first were used as an open and practical transmission media for voice and low-rate data transfers. Later, they have been initiated for higher bandwidth with the technological advances in wireless networking standards, especially after 1999. The idea of integrating emerging WLAN technology into military operations is considered as revolutionary. The use of WLAN has been three to four years in the commercial applications like Internet Hotspots, even for the developed countries. Wireless Local Area Networks established by the Army, will

provide the sharing of proper tactical and operational military information with the different levels of Headquarters and make the command and control of the units easier in the field.

After having a thorough examination of the capabilities and limitations of the three main standards of WLANs, IEEE 802.11a, b and g, the answers of the following questions should be considered:

- What key security issues do you need to be aware of before deployment?
- How will you manage the wireless LANs?
- How do you choose the right system for your organization?
- How do the features of wireless LANs influence network topology?
- What do you need to deploy a network?
- How should the logical network be constructed for maximum mobility?
- What do you need to look for in a site survey to make a deployment successful?

Deploying a wireless LAN is a considerable undertaking. Significant planning is required before touching the hardware. Deploying a wireless network is not simply a matter of identifying user locations and connecting them to the backbone. Wireless LANs are much more susceptible to eavesdropping and unauthorized access. Working to mitigate the security problems while offering high levels of service makes large wireless LAN deployments topologically more complex, especially because solving security problems means that a great deal of integration work may be required to get all the different pieces of the solution working in concert.

Beyond considerations due to the physical environment, wireless networks often extend an existing wired infrastructure. The wired infrastructure may be quite complex to begin with, especially if it spans several buildings in a campus setting. Wireless networks depend on having a solid, stable, well-designed wired network in place. If the existing network is not stable, chances are the wireless extension is doomed to instability as well.

### *5.8.1 Physical Network Planning*

Physical structure of the WLAN includes the existing cabling and the cabling requirement for access points and antennas in wiring closets or other hidden locations. Wi-Fi systems utilizing the various IEEE 802.11 standards (802.11a, b, and g) were designed to operate in a typical LAN environment. The main problem with a radio frequency wireless connection is signal containment. With proper network design, the signal can be mostly contained inside the building by locating access points properly and by adjusting the power output levels of the access points.

Wireless stations communicate with a MAC address as if it were fixed in place, just like any other Ethernet station. Instead of being fixed in a set location, however, access points note when the mobile station is nearby and relay frames from the wired network to it over the airwaves. It does not matter which access point the mobile station associates with because the appropriate access point performs the relay function. The station on the wired network can communicate with the mobile station as if it were directly attached to the wire.

### *5.8.2 Logical Network Planning*

The number of IP addresses that will be set aside for wireless users should be planned and a large enough address block should be available in advance. If the necessary IP address space is not available, it may mean cutting back on the level of seamless mobility on the wireless LAN.

### *5.8.3 Considerations for The Current Environment*

The first step of deploying Wi-Fi in a complicated environment is to find out what is already happening in the wireless environment. First, it should be looked at the current infrastructure including the networks and the systems that are in place and the physical environment of the area where RF use is intended. The age, effectiveness

and expected lifespan of existing systems and facilities all play important roles in selecting the wireless system that will best meet current and future needs.

A number of factors can affect radio propagation and signal quality. Building materials, construction, and floor plan all affect how well radio waves can move throughout the building. Wood floors can cause floor-to-floor interaction between access points. Ensure channel selections are appropriate for vertically adjacent access points. Interference is a fact of life, but it is more pronounced in some buildings than in others. Temperature and humidity have minor effects. Early site visits can assist in anticipating several factors, and a detailed site survey can spot any real problems before installation begins in earnest.

Existing wired infrastructure should be examined carefully, assuming the WLAN is an extension of or overlay on an installed wired LAN. It is also required more importantly to learn what new equipment and what integration effort will be necessary to make LAN and WLAN work together seamlessly.

### *5.8.4 Site Survey*

Before implementing a WLAN, it is useful to conduct a site survey. There are countless things in the physical environment that could impact the extent and quality of the wireless coverage, from walls and poles to metal and temperature. System designers need to obtain information on coverage, equipment placement, power considerations, and wiring requirements to ensure that users will not lose the RF signal. The way to get that information is to conduct a site survey So that they can access to their data as they move around facility.

Too many companies are trying to do their own installs with only the most rudimentary understanding of the equipment and of RF technology. Many as a result are having problems. Some of the mistakes they make are eminently avoidable. Setting up office WLANs using 2.4 GHz frequency requires a professional approach.

Every CIS manager can do a site survey. For the first RF device installations, it is strongly recommended to have an expert who has experience to handle it. If the position of access points and selection of antennas does not provide optimum throughput everywhere, users complain about poor performance because sometimes coverage is so poor there are small "dead zones" in the office with no connectivity at all. Wireless vendors and value-added resellers can usually provide this service. Some manufacturers offer free site survey software with their access point, or it may be purchased for a nominal fee. Utilizing the site survey utility includes establishing a two-way data network using both stationary and mobile devices at various points within the proposed radio coverage area. An assessment of access point signal strength using various antenna and access point configurations helps to determine the number and placement of access points required to provide proper radio wave coverage.

The site survey serves as a guide for the network design and for installing and verifying the wireless communication infrastructure. It also helps customers clearly understand the impact of the addition of wireless local area networking on their overall networking and system requirements. It determines whether a site has unusually high interference issues to resolve, or the capacity is greater than anticipated. Finally, a well-done site survey enables accurate quotes on equipment requirements to guide financial decision-making.

### 5.9 Future Probable Wireless Policy

This policy is based on the newly submitted directives and assigns responsibilities for the use of commercial wireless technologies, devices and services in a military environment. It directs the development and use of the general knowledge experienced and promotes the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the Army. Firms deploying WLANS must put appropriate policies in place for administering and securing their wireless networks.

Military units can deploy with the tactical reasons in requested time and place. The rapidly changing state of wireless technology requires that a dynamic and flexible policy be adopted. Army and the companies that will set WLANs should be more proactive in about establishing a corporate policy for the infrastructure, usage, and security. These policies are based on the experiences, written documents and directives. They should be aligned with the deployment of an approved and secure WLAN to critical areas. A sample WLAN policy can be outlined below together with the military and business rules. These rules serve as the foundation for implementing a standard WLAN. This is to ensure that a consistent approach and methodology is employed across the critical organizations (Air Defense White Paper, n.d).

### *5.9.1 WLAN Usage*

Organizations must first define the proper usage of WLANs. This includes the applications run across the network and the main APs and user locations in the enterprise. These methods can help to determine an average user profile. A detailed site survey gives an idea of the number of users in the access points. The largest coverage with the least number of APs is the ideal plan.

### *5.9.2 Applications*

Wireless LANs provide suitable platforms for many applications like connecting to corporate email accounts and surfing the Internet. One of the most important causes of WLANs could be giving a fast Internet access to users like Public Hot Spots. Another application request is VoIP (Voice over IP). WLANs can provide an effective voice communications ability within the coverage area as Cellular phones offer. However, network performance is significantly hampered by the large amount of these two WLAN activities in the area. Therefore, some organizations limit their wireless LANs usage for connecting to email and the Internet. In addition to security concerns, organizations may choose to prohibit access to classified information and related applications from the WLAN bandwidth across another WLAN. Bandwidth-

intensive applications and network misuse, such as downloading of MP3 files, can significantly drain the network and limit the wireless LAN's ability to serve multiple users.

### *5.9.3 Roaming*

Some wireless LAN infrastructure allows stations to seamlessly roam from access point to access point without dropping the connection. However, network roaming introduces security concerns that arise from the station not authenticating itself to the new access point. Organizations should evaluate the benefits of roaming and weigh them with the security risks coming from the roaming policy for their wireless LANs.

Network managers should make a layout plan of their wireless LANs and determine which stations can connect to which access points. Some stations should only connect to a single access point or a set of APs in the area. For example, a manager may need to connect to the access points in the building or corporate campus and an executive who often visits offices and organization facilities in multiple locations may ask for connecting to the access points at all sites.

Apparently, there are several ways users will be able to roam securely and seamlessly among access points in 802.11 wireless LANs. Wireless LANs provide mobility through roaming capabilities, but this feature comes with a price. The 802.11i security standard, ratified in June 2004, makes a couple of provisions for this capability.

While Layer 2 roaming refers to the user's capability to roam from one AP to another without crossing router boundaries (within the same IP subnet), layer 3 roaming refers to the user's ability to roam across router boundaries as they move about the enterprise corporation. One of the implementations for layer 3 roaming can be achieved through the renewal of the Dynamic Host Configuration Protocol

(DHCP) lease for its IP address. This can be undertaken either manually or automatically.

Mobile IPv6 (MIPv6) is a protocol developed as a subset of Internet Protocol version 6 (IPv6) to support mobile connections. MIPv6 is an update of the IETF (Internet Engineering Task Force). Mobile IP standard (RFC 2002) designed to authenticate mobile devices using IPv6 addresses (Mobile Networking Through Mobile IP, 2004). MIPv6 allows a mobile node to transparently maintain connections while moving from one subnet to another.

### *5.9.4 Off-Site Use*

The widespread growth of wireless network technology with new laptop computers forces organizations to decide with where and what types of networks employees are allowed to connect. The growth of public WLANs like Internet hotspots gives the users an opportunity for convenient connections outside the office. However, these public networks offer little security and potentially attract hackers to attack into the network. Stations are susceptible to accidental or malicious associations from neighboring networks.

### *5.9.5 Network Configuration*

Service Set Identifiers (SSID) of APs should be changed from default settings and renamed against for unauthorized users, so that they cannot decide easily which WLAN to connect. Larger organizations will require complex filtering and use remote authentication dial-in service (RADIUS) servers to manage hundreds of stations and dozens of access points.

System administrators can easily establish configuration profiles for all their data collection devices with some new remote configuration settings at a central computer. Administrators can establish networking parameters, change encryption keys and other radio settings, modify platform and BIOS parameters and completely

configure their devices in one simple operation. In addition, any software changes or application updates to the devices can be remotely handled. It's that easy, input a change, then the next time computers are booted up, the new configurations are downloaded and applied seamlessly without operator intervention.

Clustered solutions for all the major components exist, so availability is not necessarily compromised by the failure of any of the security components. Clusters are composed of several independent devices that get together and share state information among multiple machines. When any member of the cluster fails, survivors pick up the workload with no interruption. If it is decided to use either firewalls or VPNs, it should be considered using a clustered product.

One item to watch for in this area is redundancy for DHCP servers. No standard exists for synchronizing the data held by DHCP servers. However, the Network Working Group of the IETF is working towards a standardized DHCP failover protocol, which will increase the reliability of the address allocation service.

### *5.9.6 Network Performance*

Capacity status in the area should be explored and the best architectural approach in order to cover the targeted environment completely should be established. Organizations should establish policies for necessary metrics to maximize the performance of the WLAN. Traffic patterns of the wireless LAN can provide valuable operational details that can be used for the assessment of network performance degradation and overall usage.

### *5.9.7 Miscellaneous*

Real life enterprise case studies and new security methodologies that highlight common mistakes or successful WLAN deployments have to be examined. After a WLAN policy is defined, organizations must evaluate the policy's effectiveness and limitations by implementing the standards.

Network managers who supervise the policy's implementation should convince wireless users for feedback information. By conducting a formal review process, the WLAN policy should be revised to fit the specific needs of the organization. In many cases, the policy can be tightened or loosened for a greater WLAN adoption, usage, and productivity. Once the policy is revised and tuned, the policy process must be repeated to document all changes.

### 5.10 Management Systems

It is clear that a number of people aren't all that familiar with network management in general. Network management is something most users never really get to see. Issues relating to network integrity, throughput, and security are constantly monitored. They are managed in the wireless domain just as they are on wire. Separating wired and wireless system managements is not the most effective approach when you consider redundancies and lost productivity resulting from managing two separate systems. Alarms and alerts notify operations staff of problems and potential problems, some of which can be quite critical to keeping the network up.

There are several wireless network management suites available for Windows, but they are generally for enterprise networks and are very expensive. Our best bet is to learn about Linux and get started. There are many robust tools available that are free to use. Many of the products use radios to scan the air, pull data from radio chipsets in WLAN devices, and expose via GUIs and alarms what's happening on the Layer 1 wireless connection. They are more than enough in comparison to the expensive management suits used in wireless engineering.

It is very important that WLAN network should be monitored for 7x24 and managed locally or remotely from a central point. When required, a help/control desk for different inconveniences should be established to solve the problems when required. Commercial products in the market are the key components of wireless planning, implementation, monitoring, management, and security. Using these

technologies, save countless hours when troubleshooting or locating the rogue devices.

Network managers also need the creation and maintenance of documentation. The benefit of having documentation can be greater than the other costs of the system. It should be collected facility drawings and blueprints, detailed architecture documents such as wiring, the location of host systems, power outlets, and structural elements such as metal firebreaks and walls, doorways, and passageways.

### *5.10.1 Monitoring*

Encryption and authentication are an essential step to network security, because of a WLAN's uncontrolled transmission medium. WLAN traffic should be monitored to ensure that wireless link over the air is encrypted and authenticated. Stations should not be allowed for "ad hoc" modes.

## 5.11 Conclusions

WLAN integrated with existing military communication network infrastructure has significant benefits, such as mobility and flexibility, higher cost savings, and less manpower to install, operate, and maintain the network. Therefore, it is accepted that WLAN technology and security has reached the suitable maturity for military operations.

In conclusion, Army and critical organizations are ready to use WLANs with the required security standards. Based on the official written documents and personal experiences, this standard policy model can be used as the fundamental concept by the organizations that will establish a WLAN. System and network managers can validate the use of WLAN with this sample policy and use it as a template checklist. Expenses for the companies advocating the corporate to build their WLAN infrastructure can be mitigated to a reasonable level in the limit of network managers' cost estimation.

Developing such a wireless plan for the military and mission-critical organizations, channel all expertise into an official step-by-step guide. It provides more information and tools than any book. It gives detailed tasks and action steps for each phase of the plan.

# CHAPTER SIX
# SECURITY CONCEPT

## 6.1 Introduction

Security conscious enterprises fortify their mission-critical WLANs with a layered approach to security that resembles the accepted security practices of wired networks. In this chapter, an overview of current WLAN security issues will be provided. An analysis of how emerging wireless technology and security standards have evolved to meet the requirements for a secure WLAN implementation will be presented. WLAN technology and security has evolved and improved over the years to mitigate the present security vulnerabilities.

Army has prohibited connecting wireless communication devices to certain mission-critical networks. Wireless communications are more susceptible to attacks and malicious uses since information is transmitted over the air. Furthermore, interference from the nearby WLANs and different sources using the same frequency cause great vulnerabilities. Exploiting these security weaknesses in order to reach the critical data through the network can be harmful to national security. However, one can plan and successfully contend with security risks and threats in the wireless deployment.

In this chapter, the current limitations of security protocols associated with 802.11 networks will be first reviewed. A general model that will help to understand how the current infrastructure of the WLAN affects the security policies for the corporation, will be developed. This model is general enough to cover the necessary security policies at different OSI layers of Wireless LAN.

## 6.2 Wireless Security Concerns

Army regulations and security directives are mandatory and binding for military units that have determined that certain information be protected via cryptographic

means. Default 802.11 security features do not meet these standards. From the most basic security mechanisms to the latest authentication and encryption protocols, military organizations need to utilize the highest security that is possible. The more security means that the network is more protected. This gives network managers enhanced confidence in the safety of all data.

Wireless LANs have been subject to a number of security concerns. The two main goals of wireless LAN security planning are ensuring adequate access control and preserving the confidentiality of data as it traverses the wireless network. Security requirements may be dictated by legal requirements or the legal threat of unauthorized data disclosure.

### 6.3 Security Policies

An organization can remedy many of these issues by admitting today that WLANs must be secured. Emerging best practices for WLAN deployments begin with the recognition that WLAN access demands at least the same strong security measures as remote access. Begin with an appropriate use policy that prohibits unapproved deployment of access points. Continue by making use of the group authentication and privacy measures built into WLAN equipment, but be aware that these features have known vulnerabilities and by themselves do not provide adequate protection. Adopt a layered approach to security. Use a Virtual Private Networking solution on top of WLANs to enable user authentication and provide data confidentiality and integrity through encryption. Take additional measures to protect all mobile computers with personal firewall and anti-virus software, and in certain situations, consider file encryption and boot level passwords. These latter measures may protect the organization from attacks following laptop (or PDA) theft.

Even with these measures, organizations should seriously consider segregating WLANs from trusted networks. It's better to treat all WLAN users as potentially hostile and impose the same constraints like remote access and teleworkers. It's also popular to place WLAN users in a demilitarized zone (DMZ), so that new access

controls uniquely can be assigned to these users. When more hurdles are placed between the mission critical data and intruders, the more intruders will seek other, easier targets.

Policies should be established and enforced to prohibit ad hoc networks together with the network configuration essentials. Because “ad hoc” networks can allow a user to transfer private corporate documents and intellectual property to unauthorized users without going over the corporate network. Enterprises should enforce a policy that prohibits anyone from installing an AP which is not approved and configured by the network managers of the organization. Enterprise wireless LAN deployments should be based on enterprise-class access points that support the advanced security and management settings.

In order to provide interoperability among the different Services (Army, Navy, Air Force) WLANs must conform to the following common profile:

1.PKI certificates improved by National Cryptology Agency,
2.Encryption algorithms nationally approved,
3.Hardware Crypto usage in both ends,
4.IPSec (Secure Intranets)

Organizations and agencies should not undertake wireless deployment for essential operations until they have examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations. Agencies should perform a risk assessment and develop a security policy before purchasing wireless technologies, because their unique security requirements will determine which products should be considered for purchase.

Agencies must actively address security risks to protect their ability to support essential operations, before deployment of wireless networks. Deploying equipment with “factory default” settings, failing to control or inventory access points, not implementing the security capabilities provided, and not developing or employing a

security architecture suitable to wireless environment (e.g., one with firewalls between wired and wireless systems, blocking of unneeded services/ports, use of strong cryptography). Agencies should also be aware of the technical and security implications and wireless and handheld device technologies.

Finally, even when governmentally approved cryptography is used, additional countermeasures such as tactically locating access points, ensuring firewall filtering, and blocking and installation of antivirus software are typically necessary. Agencies must be fully aware of the residual risk following the application of cryptography and all security countermeasures in the wireless deployment.

## 6.4 Multi-layer Security Concept

With the adoption of WLANs by the military units, the authentication and authorization rights in order to deploy different regions and secure them correctly have gained top priority.

In this research, the current limitations of security protocols associated with 802.11 networks will be reviewed. A general model will be developed in order to understand easily how the current infrastructure of the WLAN affect the security policies for the corporation. This model is general enough to cover the necessary security policies at different OSI layers of Wireless LAN. The more authentication factors in use, the more secure the authentication. Resources requiring strong protection generally require strong or multi-factor authentication.

### *6.4.1 General*

IT managers have been forced to sacrifice key requirements to confidently and securely deploy WLANs. Deploying a pervasive WLAN, requires network managers must thoroughly examine their overall security architecture and deployment goals. They also have to consider the unique requirements of securing the RF medium, controlling network access and protecting applications and data. Therefore, the Army

should have the intention of a comprehensive wireless security—a unique multi-layered approach to wireless security frame (Figure 6.1) from location to application. Additionally, this fortified wireless security model enables organizations to easily comply with government privacy regulations (Defining the Requirements for Third-Generation Wireless LAN Security from Location to Application, 2004).

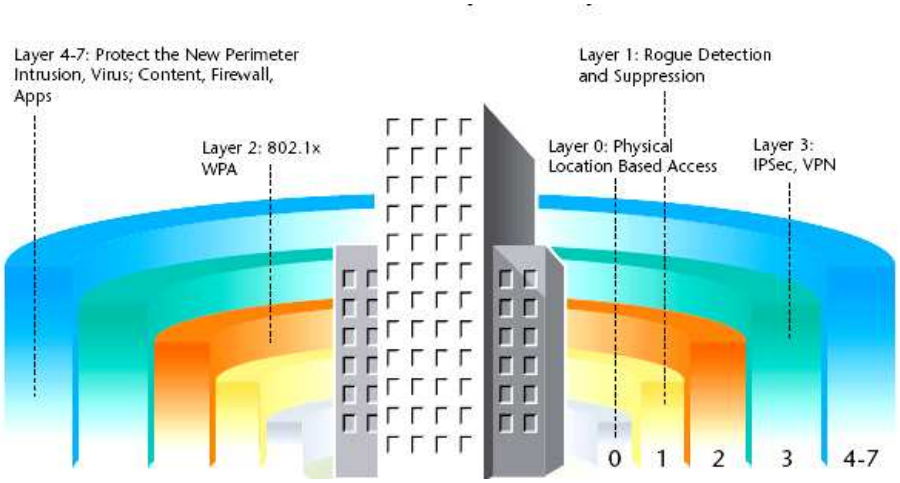


Figure 6.1 Multi-layer Security

### *6.4.2 Layer 0: Physical Location*

The most basic physical security for a wired building network is the building itself. With wireless, it is as if Ethernet connections have moved outside the building walls. There is no limit of entry points. Users can access the RF if they are within the coverage area. Unauthorized wireless devices may associate with the corporate WLAN. The ability to control users' access to the WLAN by physical location is critical.

It has to be used innovative location-based access policies in order to govern access to the WLAN. IT managers set up different "security zones" and then grants users access by these zones, such as "the first floor" or "Intelligence department". For example, HQs Security Chief may refuse wireless access to any user outside the building perimeter. Access policies apply to all higher layers of security framework,

including access to the RF spectrum, authentication and encryption, VPN and applications.

### *6.4.3 Layer 1: Detection and Protection of RF Spectrum*

Uncontrolled wireless devices can leak information, cause network downtime, reveal confidential data, and expose vulnerable access points to the outside world. A rogue is an unauthorized AP or user who has plugged into the wired side of the network or penetrated the WLAN RF space. An attacker may engage in surveillance, launch a man-in-the-middle attack, spoof MAC addresses. While rogues are typically thought of as malicious attackers, employees also can inadvertently open up security holes simply by plugging APs into the Ethernet jacks in their offices.

The most cost-effective approach is to use WLAN monitoring tools which periodically scan the RF channels to detect unapproved users or APs. However, rogues can "hide" if the APs don’t scan across all channels. If the APs do scan all channels, user communications with the AP will be interrupted for the duration of the scan. Instead of this, Land radars designed for this purpose can provide a continuous monitoring and wireless service on the same AP pool. WLAN Radar compares the AP RF data according to the deployment plan. If it detects an unknown or rogue AP or user, Network manager stops the rogue APs, preventing them from creating a security breach.

### *6.4.4 Layer 2: 802.1x Authentication and Encryption*

Authentication and encryption are fundamental forms of security, protecting network access and ensuring data privacy. Army should choose the most suitable method for its task and risk profile according to the current written and approved directives in the frame of NATO Standards and National rules.

Preventing unauthorized access to sensitive mission-critical wireless networks is a key requirement. 802.1x will provide more authentication and access control for APs

through the use of extensible authentication protocol (EAP), which is a set of messages for authentication negotiation and authentication transport method between client and server (IETF) (Secure Architectures for wireless LANs in the enterprise, 2004).

One of the other applicable access control mechanism that will be used can be a dongle, which is a simple security device, connected to a computer port in order to verify that the program is not a legal copy. This device can carry an EPROM (Erasable Programmable Read Only Memory) which is a 64 or 128 bit ID number. When the user plugs this handy device into the Wireless module, and enters the right PIN number, the transmission begins and asks the AP whether the ID number is true.

Army directives should dictate that strong authentication, non-repudiation, and personal identification are required to access the classified military network mainly in accordance with the National Public Key Infrastructure (PKI) format. The PKI implementation plan for wireless systems is being improved by National Cryptology Agency. The policy should go on to state that Identification & Authentication must be implemented at both the device and network level.

For encryption, Army and the corporations use the approved algorithms and devices. Together with nationally approved algoritm or commercially accepted algorithms, Temporal Key Integrity Protocol (TKIP) provides stronger encryption. TKIP changes the encryption key with every packet, eliminating the possibility that an attacker can decipher the encryption key. Advanced Encryption Standard (AES) with the 128-bit, 192-bit, or 256-bit encryption algorithms, the strongest exportable encryption, built into the hardware will be available as the standards are adopted and clients become available. AES use required in processing, encrypting, and decrypting data could impact operations. However, 802.11g implemented with IEEE 802.11i using AES encryption will satisfy critical wireless encryption requirements.

802.11i also referred to as Robust Security Network (RSN) is designed to address all the security issues associated with 802.11a, 802.11b, g and WEP shared key

encryption. This standard includes two parts: the AES for encrypting WLAN traffic and IEEE 802.1x Port-based network authentication standard for WLAN user authentication and key management (Atheros Communications, n.d).

### *6.4.5 Layer 3: VPNs*

Because of security concerns, many companies do not want APs in the trusted domain, so that they establish a VPN tunnel between the client and VPN server within the network infrastructure. Companies use IPSec VPNs to ensure data privacy and protection in accordance with their privacy and security requirements. If all client devices in the same network do not support 802.1x in layer 2, VPN performed at layer 3 provides authentication and encryption.

But, applying the wired VPN model to wireless VPNs requires additional hurdles, such as, larger scale of VPN users, service reliability and the ability to support multiple classes of service. The mobility of WLAN users causes performance bottleneck in the central VPN server. Installing and managing VPN client software on a large number of clients incurs a significant cost. If wireless clients dynamically download the VPN client from a central controller, which is a web server, per-user authentication and distribution of IPSec pre-shared keys can be taken before any user data is transmitted. Wireless VPNs must provide consistent, and reliable service, because VPN connections can be terminated due to long hand-off times as clients roam between APs in a WLAN. Using VPNs should not negate the use of QoS for VoIP and other real-time applications.

### *6.4.6 Layer 4-7: Unified Security*

Since mobile clients can travel and connect to internet hotspots and different networks, every mobile client becomes an entry point into the network. With an infinite number of entry points, a WLAN policy must provide comprehensive and adaptive protection against multiple types of security breaches and attacks at the wireless edge. Protecting networks and applications against viruses, worms, DDoS

and other network attacks at one location in the enterprise is inadequate. However, placing multiple point products for different protection elements, including intrusion detection and prevention systems (IDS/IPS), firewall, virus scanning and application-layer security, at many points, is too complex to be considered cost-effective or scalable.

A unified security approach providing comprehensive Layer 4-7 security must be provided at wireless edge aggregation points, where the WLAN connects to the network core. Setting up a secure WLAN, isolating it from the wired network delivers a coordinated and correlated response to attacks. Network managers can set policies, user access controls, security controls and virus updates from a central console. Technicians do not have to be dispatched to troubleshoot problems or even update software in WLAN devices in remote locations.

In a wireless environment, a system that sweeps the frequency spectrum monitoring for intruders is necessary. IDS devices monitor systems to detect attacks and intrusions by examining traffic and suspicious activities on the host devices or network, in order to alert operators. Operators can then take appropriate steps to respond to any alerts generated by the IDS. IDS systems are grouped into Host Based IDS (HIDS) & Network Based IDS (NIDS).

IPS (Intrusion Protection System) systems provide additional protection against attacks by automatically reconfiguring the network and/or host to counter an attack. They should be deployed in any mission-critical WLAN environment for real time network adjustment to secure systems under attack. However, IPS technology is still in its very early stages of development.

Firewalls control communication by allowing or denying traffic based on predefined rules using access control. Firewall should be deployed for added protection of the WLAN infrastructure.

The wireless environment provides plenty of vulnerabilities. For example, directional antennas have back lobes. Even if they are pointed toward the interior of the warehouse, a certain amount of energy is radiated out the back. RF signals from the antennas mounted on the interior ceilings may also extend significantly beyond the intended edge of coverage. A more directive client antenna will extend coverage significantly beyond the limits indicated by the site survey, leaving data sent available to interception.

It has to be ensured true 24/7 availability and users satisfaction by learning about the management, back-up, archive services, anti-virus software and software updates.

### *6.4.7 Current Security Issues for WLAN*

Agencies should be aware that physical controls are especially important in a wireless environment. Agencies must enable, use, and routinely test the inherent security features, such as authentication and encryption that exist in wireless technologies. Finding a wireless network is easy, because all wireless networks announce their existence, so that, potential clients can link up and use the service provided by this wireless network. The 802.11 beacon frames used to broadcast network parameters are not encrypted. This means the network parameters are available to anybody with an 802.11 card and an antenna. A hacker can launch an effective attack to a wireless network with a high-gain antenna looking for available access points. As soon as a WLAN is located, the only obstacle to obtain 802.11 network access is to get through the WEP (Wired Equivalent Privacy) (The formal WEP specification, n.d). if enabled. Wireless security has initially evolved from this inadequate security option in 1999. This original wireless security protocol, used 64-digit and 128-digit keys encrypted using an algorithm called RC4. With WEP, each client machine was assigned one key per session. WEP was cracked in the summer of 2001 and has since been a weak link in the wireless security chain (A wireless LAN security glossary, n.d).

WEP is problematic, but it may be better than running open access points. In many environments, though, WEP should be disabled. With large numbers of users, WEP is just another configuration item to get wrong. Deploying WEP may also complicate roaming between access points. It has to be carefully considered the limitations of WEP and deployed additional solutions to enhance: Wireless middleware when implementing complex networking projects are necessary . In addition to application management, middleware products often offer access control and encryption mechanisms that counter the issues of 802.11 WEP. The supporters are probably referring to dynamic WEP with LEAP or PEAP authentication. Although dynamic WEP is not the ideal solution, it is more secure than static WEP for two reasons. First, these systems are typically set up to re-authenticate each user every 30 minutes. During the re-authentication process, the access point produces a new WEP key that is used until the next re-authentication. Second, a different WEP key is used for each station, so the communication of another station cannot be intercepted. The use of dynamic WEP, except as a short-term solution until the system could be upgraded to WPA with RADIUS, would not be recommended.

However, many vendors and network administrators did not implement WEP. Instead, they chose an alternative security solution called MAC-address filtering. Basically, MAC address filtering was used by the access points to check the physical addresses of the connecting devices as part of the initial network access procedures in order to ensure that the station is already in the list of good MAC addresses. Although MAC address filtering was widely deployed, it was not able to provide a serious security solution. First, it lacks the validation of the system software running behind the good MAC address, which may include some harmful programs such as, eavesdropping programs, spyware, or Trojan horses. Second and the most important reason is that MAC addresses can easily be changed at present.

Easy deployment of WLANs also causes another security problem. A user with little knowledge of the available security vulnerabilities can set up a “Rogue” access point, which easily provides an attacker with open access to the wireless network.

To combat the security glitches in WEP, 802.11 working group adopted the 802.1x standard. 802.1x provides “per-port user authentication” that requires user-authentication to ask for access to the network, using the Extensible Authentication Protocol (EAP) built into 802.1x. Transport Layer Security (TLS) method creates a secure session before sensitive information and encryption key are sent over the connection. In the IEEE's 802.1x, EAP is encapsulated in LAN or WLAN traffic, providing the mechanism for verifying the identity of a user to RADIUS or other authentication server. It supports many authentication methods, including Kerberos, public-key authentication, and smart cards.

Wireless vendors developed Wi-Fi Protected Access (WPA) to increase the encryption by using another keying mechanism with Temporal Key Integration Protocol (TKIP), which changes the key several times during each session by making keys more difficult to be cracked. WPA adds a strong message-integrity check and allows for authentication using 802.1x (A wireless LAN security glossary, n.d)

A major part of WPA security was to come from a stronger algorithm called the Advanced Encryption Standard (AES), the replacement of RC4. It was developed for the U.S. military by the National Institute of Standards. However, developing the protocols using AES and bringing vendors together to decide on the specifics has taken a lot of times. So that, vendors continued using TKIP instead of AES for most released products.

The IEEE has not approved the latest version of 802.11i which vendors and integrators still refer to as WPA2, until June 2004. Additionally, independent organizations prefer using encrypted certificates and certificate servers that validate their authencity based on Public Key Infrastructure Structure.

It will be necessary to employ higher-level cryptographic protocols and applications such as secure shell (SSH), Transport-Level Security (TLS) or Internet Protocol security (IPSec) with military modules and associated algorithms to protect

the information, regardless of whether the nonvalidated link security protocols are used.

### *6.4.8 Security Implementations*

Authentication is the process of verifying that someone or something are who they say they are before they are granted access to protected resources. Such resources may include software applications, computing facilities, printed data, printers, or physical access to facilities and materials.

Most discussion of authentication concentrates on online authentication, but offline methods of authentication are also around. Such offline methods of authentication include checking for valid forms of identification, or having security personnel check and recognize an employee's face before admitting them into the building or restricted military area. Online authentication tools include user IDs and passwords, smart cards, security tokens, and biometrics.

For example, a device that saves users from having to create or remember secure passwords. The system uses a key fob that plugs into a computer USB port and generates a new password each time a user logs in. To authenticate themselves during an online session, users enter the serial number on the back of the device and the password or code that appears on a small LCD display.

#### *6.4.8.1 Access Point and Access Control*

APs and access control require a method whereby users are identified for this access. This could be a process for the service and provides relevant data for this access. This may be assigning a username and password for login access, or it could be identifying the MAC address of the wireless network interface card (NIC) the user owns, or both. While the complete specification of a telecommunication database is very complex and has many elements that are specific to the organization, a simplified relational database structure would include tables that identify the user,

their MAC address, and the wireless access points. A skeleton of some of the relevant relational database tables is shown in Figure 6.2.

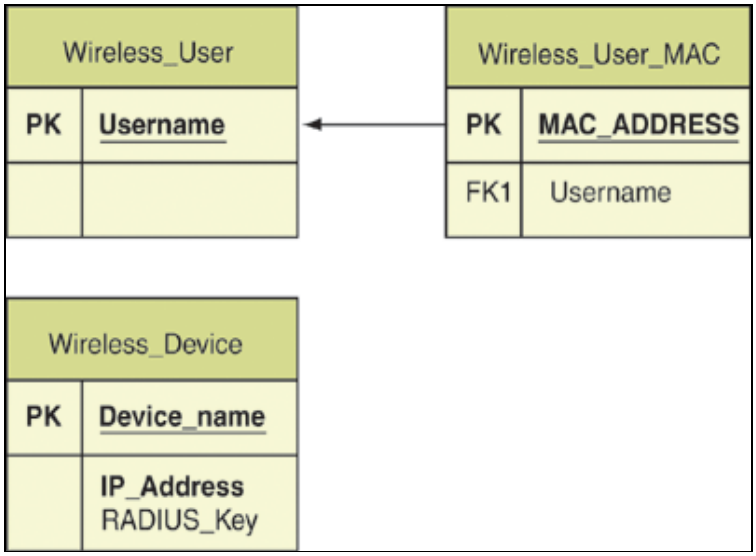


Figure 6.2 Authentication Records in Relational Databases

Shutting down access of a wireless client can be done a few different ways. The best way to disconnect a client from the network is blacklisting the MAC address of the client. A more sophisticated approach would be to re-direct traffic intended for the user to another machine (which is similar to a DOS/Middle Man attack hackers use). These types of reactive measures are not done via a laptop, but software or manual configuration of the routers.

*6.4.8.2 RADIUS*

The model for RADIUS is that a network access server (NAS) will have users connecting to it. The NAS then receives authentication data from the user and sends requests to a RADIUS server based on the data to determine whether the user is authentic and is authorized for the network; hence, the NAS is a RADIUS "client". The NAS encrypts communication with the RADIUS server using a shared key (which can be client-specific). In Chapter 7, the application sample reviews the configuration of a RADIUS server in detail.

There is a way to cache encryption keys to sidestep having to repeatedly authenticate with a RADIUS server. The other feature is the ability to tie in with a pair of third-party applications that check client devices before letting them access the network. Without this feature, the device would have to re-authenticate and receive a new key each time it associates with a different access point

*6.4.8.3 Different Software Features*

With the release of new software using SNMPv3, Secure Sockets Layer, and Transport Layer Security, giving the web server embedded in the company's switches the ability to handle secure HTTP transactions. This way, network managers can manage switches remotely, using a web browser, without fearing that an unauthorized individual might do the same.

Comparing this to previous secure management, this involved plugging a console directly into a switch or using a telnet session. Obviously, accessing a switch over the Internet is immensely more convenient, but industrial users don't trust web management, thinking that displeased employees or terrorists might be able to get in as well. The web server can perform authentication to verify the identity of whoever is trying to access the Ethernet switch and can encrypt passwords as they traverse the Internet.

## 6.5 Conclusions

How traditional network security measures are being applied in new ways to secure WLAN access to small business, enterprise, and service provider networks were considered in this chapter.

Administrators should maintain a separate authentication system for WLAN users. When the number of users is limited, it seems reasonable, but it introduces a significant burden as the network grows. Support for external authentication databases is also necessary.

Even when governmentally approved cryptography is used, additional countermeasures such as tactically locating access points, ensuring firewall filtering, and blocking and installation of antivirus software are typically necessary. Agencies must be fully aware of the residual risk following the application of cryptography and all security countermeasures in the wireless deployment.

The latest 802.11g for wireless communication, combined with 802.11i providing advanced WLAN encryption, and 802.1x for strong authentication, can be promising enough for tactical WLAN deployments now. It should also be built, tested, and demonstrated the tunneling principles like VPN (Virtual Private Network) for transferring the IP data through the wireless infrastructure.

Any design, no matter how strong, must be regularly audited to ensure that the actual deployment is consistent with the security objectives of the network design. Inappropriate configurations may be a major source of security vulnerability, especially if wireless LANs have been deployed without oversight from security engineers (The Top Seven Security Problems of 802.11, 2003).

# CHAPTER SEVEN
# USER BEHAVIOUR MODEL/APPLICATION

## 7.1 Introduction

Because Wireless LANs are not inherently secure, and WEP is not an end-to-end security mechanism for enterprise WLANs, there is a significant opportunity for other security solutions to take the forefront in the wireless LAN security market. In this chapter, some of the possible security solutions which can be applied in a WLAN environment without requiring any proprietary solutions, will be examined.

These models will help to create a securely specific environment from the point of military aspects. Even though, there are so many standard and protocols, a different and new standard that the industry and the public can accept, is required.

## 7.2 Architecture

Different wireless security systems provided with and without encryption using Ethernet endpoints to generate traffic were installed and configured. The purpose here was to measure the products' capacity and using the Ethernet was the most efficient way to accomplish this goal.

For the software-based products, two different access points connected to an Ethernet Hub were configured. When a wireless device moved from the coverage area of one access point to the coverage area of another, it would reassociate with the new access point. The same thing could be done by using a switch and changing the subnets as well.

For the hardware-based solutions, two control servers used for authentication and centralized management and two different access points were installed and placed in the same network.

"NetIQ's Chariot" is used to run performance scripts to determine the throughput of each system. Raw, unencrypted performance between a group of end nodes on a "HPJ2610B Hub" achieving throughput of approximately 10 Mbps is measured first.

Other areas of the testing are standardized. Authentication with the Microsoft Windows 2003 Server Active Directory Policies is also tested.

### *7.2.1 Test Bed*

A test network (Figure 7.1) is created with two access-points (one is thin, the other is thick) and with a Hub. The software-based products on the servers are set up. Clients could reach the server with an only one hop over the access points. The only thing to do for running the applications, is to take the laptop and launch the web browser.

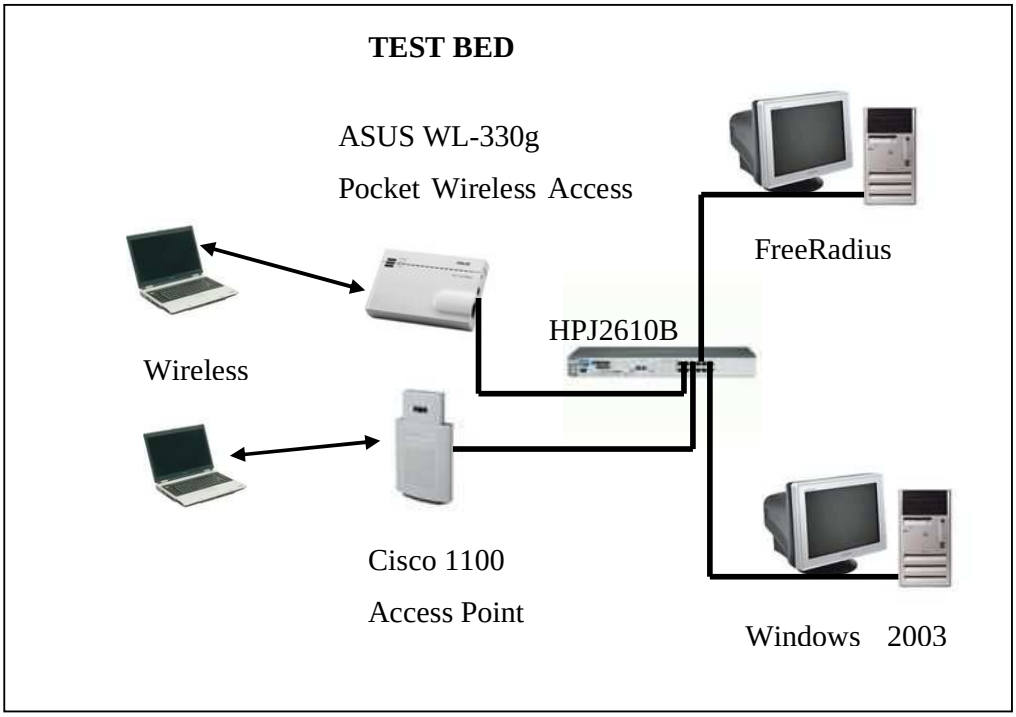


Figure 7.1 Application Test Bed

*7.2.1.1 Windows 2003 Server*

All software platforms  are installed on an Escort PIV 2.8 GHz PC with 256 MB of RAM. Server installation is easy. If there is a Windows network, this product will fit in easily with the existing Domain. The wizard guidance is used through the input of minimal configuration information. The domain or Active Directory is checked to see and authenticate clients in the wireless users group that will connect to the server. Some users are created, and added to the group, and the preliminary configuration is completed.

*7.2.1.2 FreeRadius*

An Escort PIV 2.8 GHz PC with 256 MB of RAM is used. A Linux enterprise was installed and added into the domain. FreeRadius software was downloaded from the Internet and installed with some specific features. It can readily be configured to use text-file databases with slightly different file formats. FreeRadius has a large installed base and active user community, and it is closely modeled on legacy RADIUS servers.

If the MAC address belongs to a valid RADIUS user, the MAC address is considered authorized to use the wireless LAN. RADIUS server that would support plain-text configuration files is used to ease of integration. There are two files for the purposes: One for the user database (with the MAC addresses of authorized users), and the other to identify the RADIUS clients (i.e., the wireless access points) and their associated encryption keys.

*7.2.1.3 Cisco 1100 Access Point*

This wireless LAN transceiver serves as the center point of a stand-alone wireless network or as the connection point between wireless and wired networks. It is IEEE 802.11b and 11g client designed for the enterprise office environment.

The access point uses the Cisco IOS operating system. Cisco IOS software is a feature-rich, network systems software that provides a common IP fabric, functionality, and command-line interface across the entire network.

This device authenticates users and tunnels traffic from wireless devices within its range as well as devices wired to it via Ethernet port. The device would fit in branch offices where employees come and go with laptops. Because it tunnels traffic between the wireless device and the access point, it overcomes and security concerns raised by using Wi-Fi. The access point supports 802.11b and g. They can be managed centrally.

AP automatically gets an IP address from the DHCP server on Windows 2003 Server. If the proper IP number is typed on the Internet Explorer, the following pop-up login screen ( Figure 7.2) appears.


Figure 7.2 Cisco 1100 AP Login Screen

After typing the default password in the manual, the Graphical Configuration Interface of the Cisco AP can be reached.

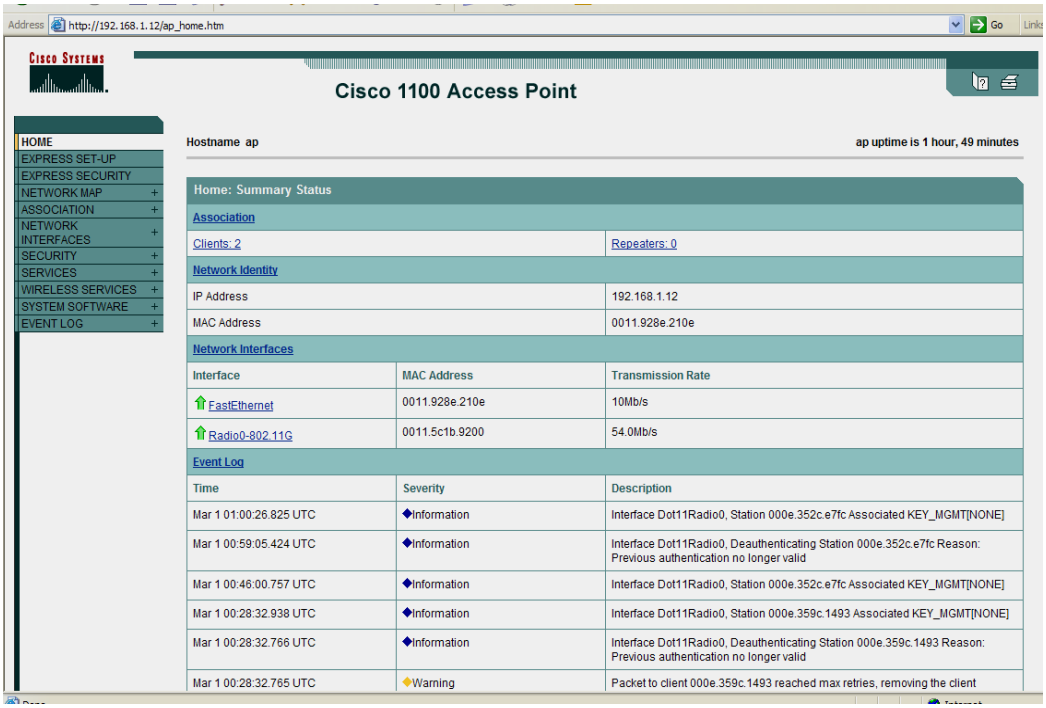


Figure 7.3 Cisco AP Configuration Interface

It can be managed and configured every settings on the Cisco AP by using the following menus:

“Express Security” provides static WEP Keys, EAP and WPA security settings via Radius Server.

“Association” gives the wireless clients on the AP (Figure 7.4).


Figure 7.4 Association Menu

“Network Interfaces” menu provides necessary information about IP address, Fast Ethernet, and 802.11g settings.

“Security” menu (Figure 7.5) is used to configure all of the security settings and specifications. “Admin Access” gives the ability to create local users and their password definitions in order to make them available to use the configuration tool.

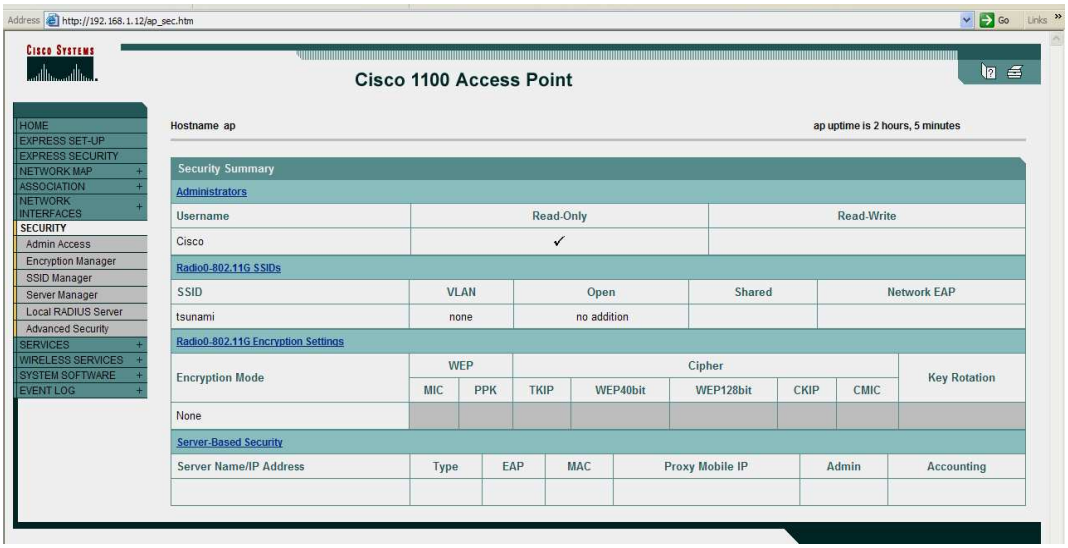


Figure 7.5 Security Settings

“Encryption Manager” arranges the encryption protocols that will be used. Settings for Radius server ( IP address and shared key) can be configured from the “Server Manager” tab (Figure 7.6).

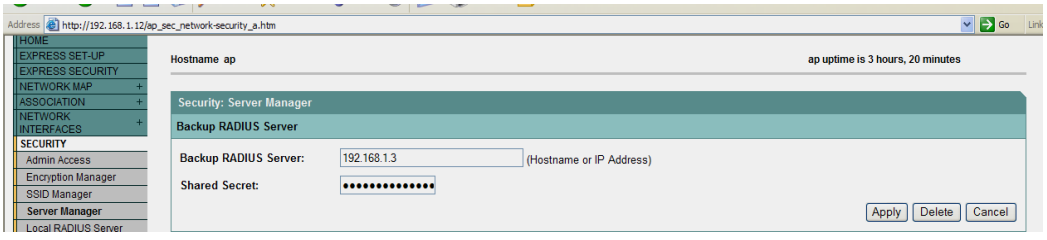


Figure 7.6 Server Manager Settings

“Advanced Security” (Figure 7.7) provides to create MAC address based authentication list.

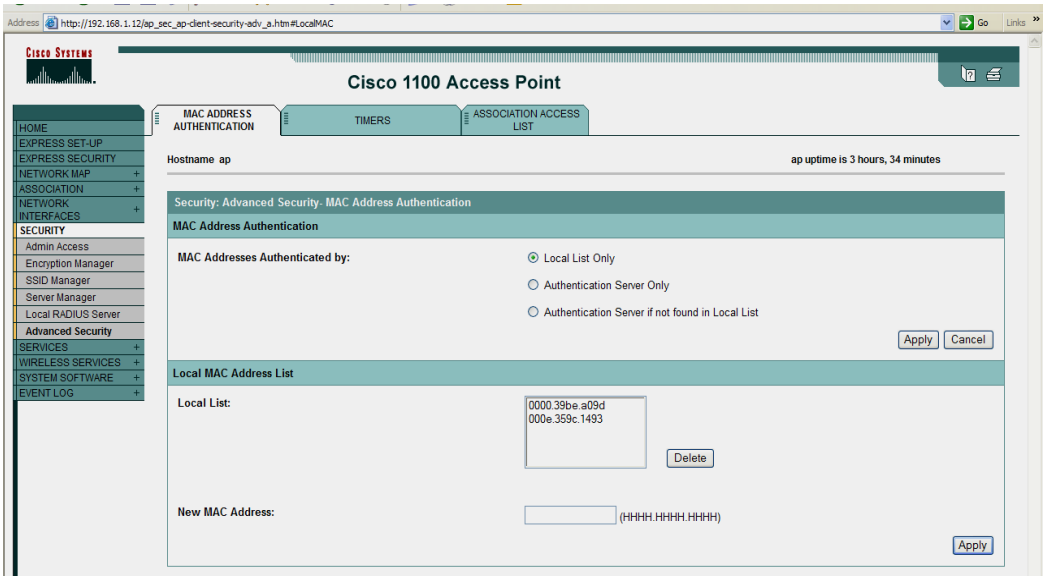


Figure 7.7 MAC Address Authentication

“Services” provides the necessary settings for the services such as Telnet, DNS, HTTP, VLAN, and SNMP.

### *7.2.1.4 ASUS WL-330g Pocket Wireless Access Point*

This is a commercial IEEE 802.11b/g wireless access point. It has a very simple setup utility program. AP supports three different operation modes (802.11b, 802.11g, and mixed). It has a two-way switch on the back. It is brought to “Ethernet Adapter” mode, and connected to a PC or Laptop to start the configuration.

If the wireless setting program is run from the “Start ->ASUS Utility->Wireless AP->Wireless Setting”, after installing the setup program, the following screen appears (Figure 7.8).


Figure 7.8 AP WL-330g Configuration Utility

After pressing the “Configure” tab, Network Name (SSID) on the next coming screen is given (Figure 7.9). This should be the same name with wireless adapter settings. Later, second tab “Encryption” is set. “Advanced” tab can be left with the default settings.

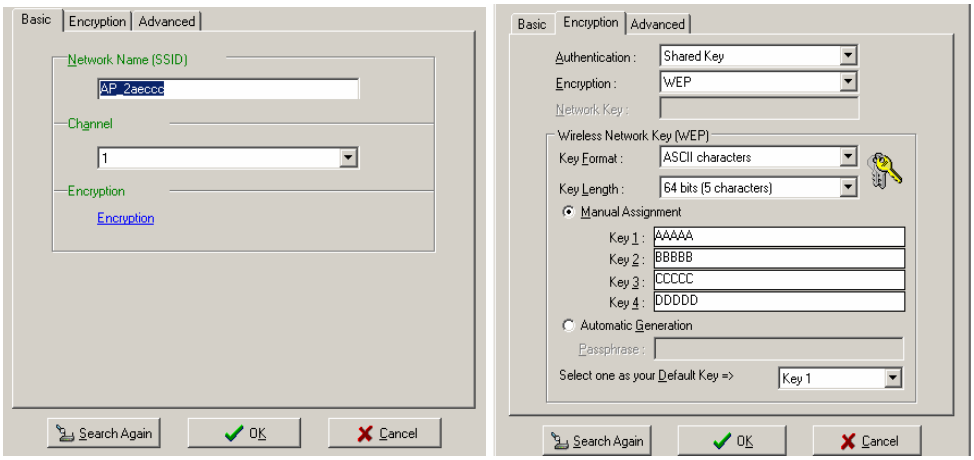


Figure 7.9 Basic Configurations for ASUS AP

*7.2.1.5 Wireless Client Stations*

A mobile P III, 1GHz Laptop with Windows 2000 (256 MB of RAM) with ASUS WL-167G USB 2.0 Wireless Ethernet Card, and an HP Intel Centrino 1.4 GHz Laptop with Windows XP (512 MB of RAM) are used. If the program is run from the "Start ->ASUS Utility->WLAN Card->Wireless Setting", after installing the setup program, the following screen appears (Figure 7.10). This screen enables the configuration of the ASUS wireless card.

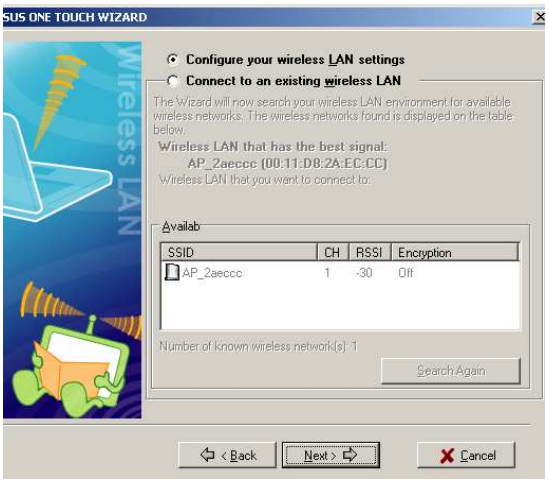


Figure 7.10 ASUS Wireless Adapter Configuration Tool

First, the SSID name and secure authentication settings (Figure 7.11) are configured.

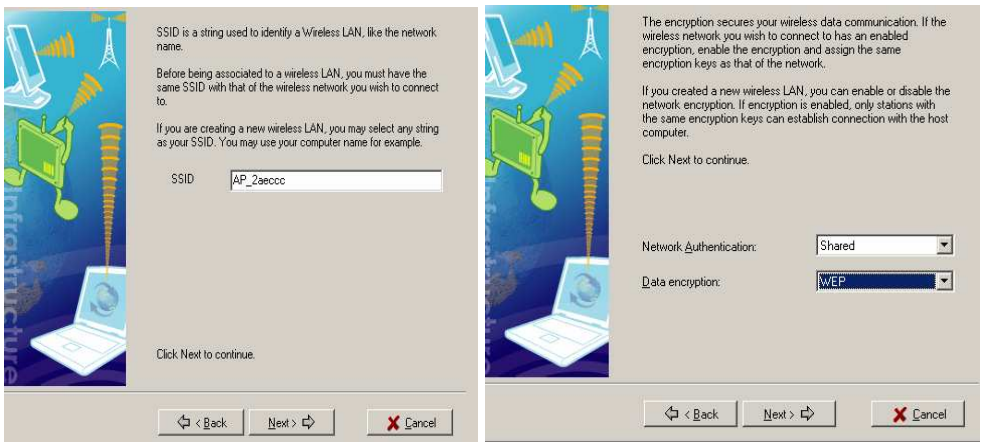


Figure 7.11 SSID and Authentication Settings

The options “Encryption (disabled, WEP)” and “Network Authentication (open,shared)” have to be decided. If WEP is chosen, the same WEP keys (Figure 7.12) with AP (Figure 7.9) should be used.

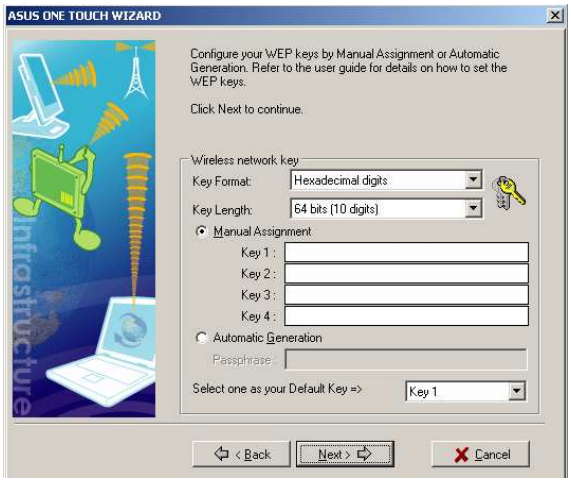


Figure 7.12 Wireless Adapter WEP Settings

Finally, TCP/IP setting is made manually or automatically from the DHCP server.

## 7.3 Authentication and Access Control

To make the wireless LAN environment easy to support while maintaining some level of access control with newly written software applications for this thesis and FreeRadius attributes, it is preferred to provide the access control with no end-user intervention or configuration. It is also preferred as little reliance on vendor-specific features offered by friendly interface tools as possible. One attribute of wireless LAN users is their inherent mobility, making DHCP an obvious requirement. So, by only supporting DHCP for IP assignment, and only allowing registered MAC addresses to be served an IP address by the DHCP server, a level of organization-based access control can be achieved.

Advantages to this approach are that it is very straightforward to implement and it makes no assumptions about either the wireless client or the wireless access point configuration. Users can authenticate on any access point managed by the RADIUS.

Access control rights are tied to the existing accounts in Active Directory of Windows 2003 Domain Controller, because Windows gives an easier time to integrate into this environment.

If there is a group of people who work for mission-critical tasks in an office, a static list of allowed MAC addresses could be configured on one access point (Cisco 1100 in this test bed), and indeed this is a very good feature to use in a residential network. However, for a network of several access points with mobile users, such a static list on all access points would be a difficult network management problem.

### 7.4 Privacy

It is found that enabling encryption hampered the performance, so some sites may want to configure encryption on an application-by-application basis. Several products support this capability, though this approach does add to the administrative burden. In the test environment, the encryption technique depends on the features of the access points. While Cisco 1100 offers WEP, EAP and WPA, ASUS gives only WEP alternative.

### 7.5 Sample Application 1 (Authentication and Access Control)

If the credentials for the user who are trying to logon to the network is already existing in RADIUS database, user gets a POP-UP screen showing the login is successful. If not, users are redirected to a Captive portal (custom redirect URL) provided by the RADIUS server. It means RADIUS does not have the credentials on the database. After the user signs up or logins with specific personal details, he/she can pass through the captive portal and everything works fine. Once authentication is complete, user and group access-control policies in the Domain Controller run and give the permission rights. WLAN users are wished to be authenticated to ensure only legitimate users gain access to the network.

To be manageable, this configuration must be dynamic, with the access points checking MAC addresses via some client-server protocol. With this feature, the access point asks the RADIUS server whether the MAC address is a valid user (with plain-text password of "NOPASSWORD"). Thus, the authorized MAC addresses can be extracted from the database and configuration files can be constructed for the RADIUS server. However, FreeRadius didn't give this ability to configure it properly. With the specific third party software tools provided, the text and graphics of the captive portal page can be customized.

### *7.5.1 Program*

Each user should run the "WLANClient.jar" file after turning on his/her PC or Laptop. This file should be placed into the "Startup" folder together with the "ClientConfiguration.txt" file. When the PC is turned on, this program runs at background. The proper IP number for the server which runs the server application program (Table7.1) should be typed.

Table 7.1 The Structure of "ClientConfiguration.txt" File

| Host_Address<br>192.168.1.2<br><br># Type the IP address given by your network manager |
|---|

If the ClientConfiguration.txt and WLANClient.jar are not in the same folder, a pop-up message appears on the screen (Figure 7.13). If a message like this is displayed, the files in the "Startup" should be controlled and the file names should be properly written.


Figure 7.13 ClientConfiguration.txt not found

But, if there is a change of format while the files are properly in the "Startup", the following message appears on the screen (Figure 7.14). It should be checked to see if it is the same as Table 7.1.

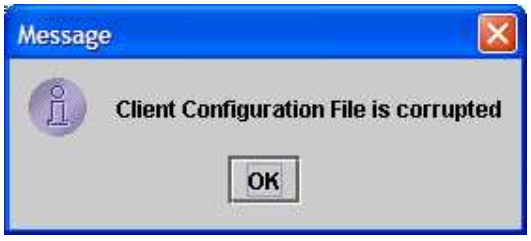


Figure 7.14 Format Change in ClientConfiguration.txt file

When the "WLANClient.jar" runs properly, user will be informed with the following screen (Figure 7.15). This screen gives the user the information of server being connected and the IP assigned.


Figure 7.15 Proper Connection Message

### *7.5.2 Results*

Many of the cheap network adapter cards and Access Points support only open and shared modes including WEP. In such devices, additional authentication techniques that will give us the users and group access control in the network are

needed. The RADIUS used as an authentication server for the proper network logins gives a screen control for administrators to monitor users and identify internal breaches of security policies.

Built-in security features of 802.11 (data link level encryption and authentication protocols) in the AP used and wireless adapter, should be used as part of an overall defense-in-depth strategy. Although these protection mechanisms have weaknesses, they can provide a degree of protection against unauthorized disclosure, unauthorized network access, and other active probing attacks.

Even though the 802.1x protocol has the considerable attention in the WLAN industry as an authentication solution, our ASUS AP doesn't support this standard. Although 802.1x may represent the future for WLAN authentication, limited client availability and interoperability issues make it difficult to implement today.

## 7.6 Sample Application 2 (Network Monitoring and Authentication Control)

This application provides a centralized configuration and status monitoring of Clients connected to the network, no matter from which AP provides the connection. It is a very simple administrative interface and can be improved by adding necessary SNMP features.

### *7.6.1 Program*

RADIUS Server acts as a separate user-defined control center. When the "WLANServerApplication.jar" program runs, it creates the following screen (Figure 7.16). This interface provides the IP address and Port number information for each connected client.

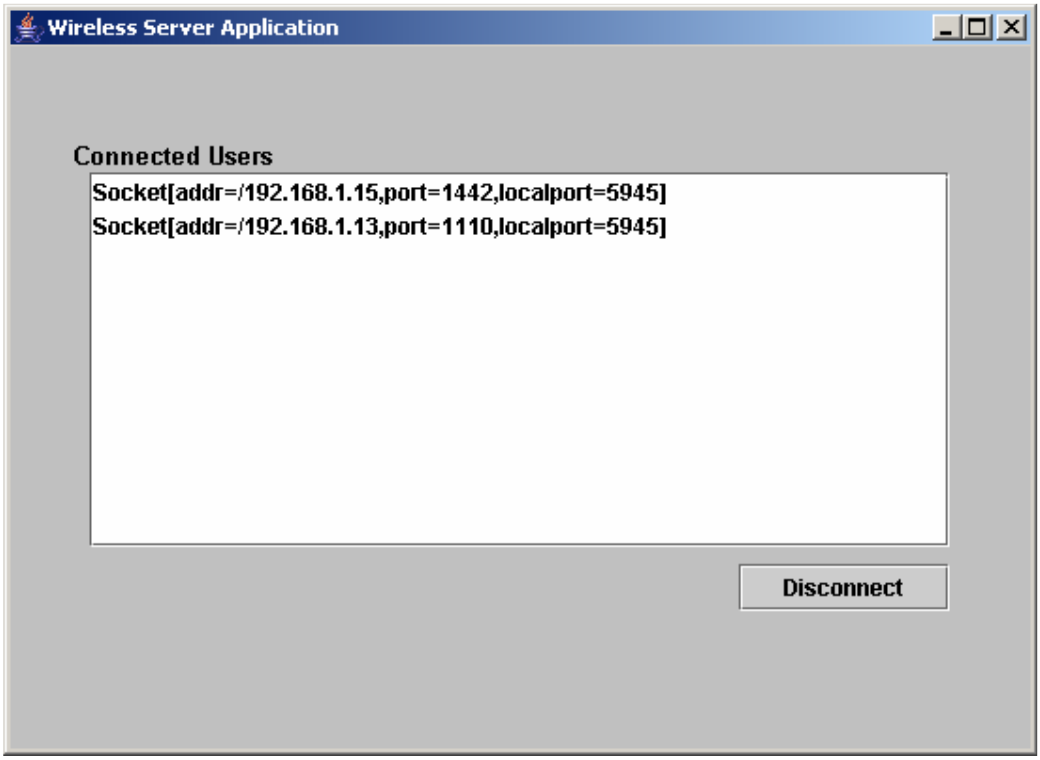


Figure 7.16 Server Interface to Monitor the Connected Clients

This program checks all the users and refresh the screen view in every 5 seconds by pinging the connected clients..

### 7.7 Paths for Application Programs

A specific folder named "*C:\Program Files\WLANApplication*" have to be created in our client PCs or Laptops, and the "*WLANClient.jar*" and "*ClientConfiguration.txt*" files should be put in this "WLANApplication" folder. Later, a shortcut of "*WLANClient.jar*" under Windows Startup can be added.

The same thing will be done in the RADIUS Server. The folder path is "*C:\Program Files\WLANServerApplication*". After putting the "WLANServer.jar", a shortcut under Startup is created.

In order to run these programs in both the clients and the server, the JAVA in advance should be installed. The URL “http://java.sun.com” will help to download and install the software.

### 7.8 Tests for Military Usage

Three wireless AP devices are tested for their effectiveness in providing key security services on a critical test network. The solutions helped with management capabilities, enhanced the security and manageability of the networked wireless devices. However, the results were not significiant from the WLAN performance point of view.

If WLAN is geographically large, but the number of users is relatively small, it may be found a better value in software licensed on a per-user basis. However, if there are many users, the hardware solutions may be more cost-effective. The products are evaluated based on their features and functionality, ease of configuration and management, diversity of client support, and the cost.

### 7.9 Required Future Improvements

FreeRadius Server does not have a user interface. Therefore, system management can only be put into practice by using the configuration files. For this reason, nothing can be performed in the run time. New administrative applications having easier and secure interfaces can be improved for the user requirements, if the necessary RADIUS APIs are obtained. The same administrative interfaces can help for different logins and back-end authentication methods.

In addition to this, network traffic data can be kept under control by using APIs in the access points and other hardware components of the network. This feature gives the ability to control traffic volumes according to bandwidth allocated to individual traffic protocols and services. By using these tools, the bandwidth consumption for each user can be learned.

A web server can be installed in order to provide a captive portal access. Users who do not have the credentials for logon in one of the RADIUS, LDAP or Active Directory databases, are redirected to this server and download the necessary applications (WLANClient.jar) by using the shared folder like a common pool. In order to provide the proper routing, a router has to be installed as well. In such an architecture:

-Router is configured to pass all the network traffic.

-Clients get an IP address from the DHCP, if they are in the perimeters of the wireless network.

-Any packet from the new user comes into the router. If the user is recorded in the database, the packet is forwarded to the required address. If not, the destination address in the packet is replaced by the address of dummy web server.

-User is recorded and downloads required applications.

-User is ready to use the wireless network.

# CHAPTER EIGHT
# CONCLUSION

## 8.1 General

The project presents the desired technology needed by the Army to fulfill the specific mission objectives to improve communications between field representatives and office personnel. The existing methods and the available technology information are included. Following the presentation are the business issues and constraints that cover many of the necessary considerations in the acquisition and implementation process.

The conclusion brings all of this information together to be presented to the case company for consideration. The included information (including appendices) will adequately provide a methodology for the company pursuing the incorporation of this technology. Additionally, highly beneficial and creative applications for this technological amalgamation will be discussed orally with the president of the case company and industry legislators.

One of the practical results of this study is that it would demonstrate the feasibility of WLAN technology working for military environment and the functionalities of the entirely new wireless concept of military units.

## 8.2 The Contributions And Main Findings

In summary, Army has prohibited connecting wireless communication devices to certain mission-critical networks. This mandate was mainly due to the huge security risks and threats associated with wireless communication. Wireless communications are more susceptible to attacks and exploits as information is transmitted over the air. Exploiting these security weaknesses to compromising sensitive military networks can be harmful to national security.

WLAN integrated with existing military communication network infrastructure has significant benefits despite these risks. Such benefits include; mobility and flexibility for mission success, cost savings associated with running wires, reduced manpower required to install, operation, and the maintenance of the network.

In this paper, it is tried to determine if WLAN technology and security has reached the suitable maturity for military operations. The evaluations were based on the former written directives and real life experiences.

Existing 802.11b WLAN technology using weak WEP encryption failed to meet this sample WLAN policy and requirements. However, WLAN technology and security has evolved and advanced over the years to mitigate the vulnerabilities, risks, and threats. The latest 802.11g for wireless communication, combined with 802.11i for advanced WLAN encryption, and 802.1x for strong authentication can be promising enough for tactical WLAN deployment.

Ultimately, a multi-layered approach of additional security safeguards like firewalls, NIDS, HIDS, IPS, and embedded security features are essential for an effective, approved, and secured WLAN implementation.

This thesis also explains what WLAN Policy means to all government agencies and what steps can be taken to ensure compliance with this policy. The implementation of the proposed architecture and the policy can be used in the places where the security is really a concern for commercial and military users.

The anticipated contributions of the proposed research to the fields of WLAN concerns, security policies, and reconfiguration features are as follows:

- A collection of information for WLANs to create a common knowledge.
- A proper standard procedure list and framework for modeling and designing a methodology to set up WLANs for corporations.

- A proper procedure for the required security policies for the subjected corporation.
- A framework for analyzing and establishing performance measures for mobile terminals.
- A process for reconfiguring the mobile terminals during roaming.

This dissertation covers details specific to wireless technologies and solutions. Even though it is in the critical side of the wireless networking, it provides the necessary background to fully understand the topics related with the wireless technology. Hence, the following list provides the highlights how network engineers and executive people (commanders of the Military HQs) might use this thesis.

- High-level senior personnel who are planning to employ wireless LANs in their organizations.
- System and network engineers when designing and implementing wireless networks.
- System administrators when administering, securing or upgrading networks.
- Security consultants when performing security assessments in wireless environments.
- Future researchers and students who are trying to understand the wireless technology.

### 8.3 Future Work

The vendors and standards community is aggressively working toward more robust, open, and secure solutions for the near future. With the evolution of multifunction, multi-network wireless devices, some of the future may be seen today. Manufactures are combining wireless standards with the goal to provide a device capable of delivering multiple services. However, each new development will present its own security risks, and government agencies must address these risks to ensure that critical assets remain protected. Largely, most of the risks can be mitigated. However, mitigating security risks requires considerable tradeoffs

between technical solutions and costs. For these reasons, it may be prudent for some agencies to simply wait for these more mature solutions.

In future wireless service provision will be characterized by global mobile access, high quality of services, and easy and simple access to multimedia services for voice, data, message, and video. In the same way a cell phone moves between radio cells, wireless devices would hop between cellular, Wi-Fi, ultrawideband and Bluetooth networks without the user being aware of the handoffs.

As the wireless industry matures, the needs of carriers are changing and many new requirements are forcing for new developments and techniques to meet these concerns.

**REFERENCES**

Air Defense White Paper. (n.d). *Wireless LANs: Six Steps for Enterprise & Regulatory Policy Compliance.* Retrieved May 22, 2005, from http://www.airdefense.net

*A wireless LAN security glossary*. (n.d). Retrieved April 4, 2005, from Techworld Web Site http://www.techworld.com/security/features/

Atheros Communications. (n.d). Building a secure wireless network. How Atheros defines wireless network security today and in the future. Document Number 991-00001-001.

Barken, L. (2003). *How Secure Is Your Network?.* Prentice Hall.

Cohen, A., & O'Hara, B. (2003). Network World. Introducing New Wireless Security.

Craig, M. (2004). *802.11g: New PHY on the block*. Retrieved August 25, 2004, from http://www.wireless.itworld.com/4246/.

Defining the Requirements for Third-Generation Wireless LAN Security from Location to Application. (2004). Meru Networks.

Geier, J. (2003). HiperLAN/2:An Efficient High Speed WLAN. Retrieved February 18, 2005, from http://www.wi-fiplanet.com/tutorials/article.php/210951.

Geier, J. (2003). *Killer WLAN Applications*. Retrieved April 10, 2005, from http://www.wi-fiplanet.com/tutorials/article.php/2175451.

IEEE Std 802.11b. (1999). *Supplement to ANSI/IEEE Std 802.11*, 1999 Edition.

IEEE Std 802.11a. (1999). *Supplement to IEEE Std 802.11*, 1999 Edition.

IEEE Std 802.11g. (2003). *Amendment to IEEE Std 802.11*, 1999 Edition.

Krolak, M.K, & Novak, M.E. (n.d). A*n Introduction to Infrared Technology:Applications in the Home, Classroom, Workplace, and Beyond.* Retrieved February,16, 2004, from http://trace.wisc.edu/docs/ir_intro/ir_intro.htm

Marvin, K.S., Omura, J.K., & Scholtz, R.A. (2001). *Spread Spectrum Communications Handbook* (1st ed.*).* McGraw Hill.

McCullough, A. (2001). Designing a Wireless Network: Understand How Wire!. Syngress.

Mobile ad-hoc network. (n.d). Retrieved April 12, 2005, from http://en.wikipedia.org/wiki/Mobile_ad-hoca_network

*Mobile Networking Through Mobile IP*. (2004). Retrieved March 12, 2004, from http:// www.computer.org/ internet/v2n1/perkins.htm.

Molnar, D. (2003). Wireless LAN Security: What Every Technology Professional Should Know.

NC3A Technical Note. (2003). NATO Network Enabled C3 Architecture Concepts For Support Of A Combined Joint Task Force Deployment. Retrieved April 27, 2005 from http://nc3ta.nc3a.nato.int/website/.

Network Project: (2005). *Wireless LAN: Regulation and Standards : Interference.* Retrieved March 27, 2005 from http://ntrg.cs.tcd.ie/undergrad/4ba2.02/ wireless/reg2.html.

Nichols, R.K., & Lekkas, P.C. (2002). *Wireless Security:Models, Threats, and Solutions.* McGraw-Hill Companies, Inc.

Nortel Networks. (2004). *Secure Architectures for wireless LANs in the enterprise* Retrieved November 24, 2004 from http://www.nortelnetworks.com/ solutions/security/collateral/.

Ou, G. (2005). *Understanding the priorities in Cryptography*. Retrieved May 30, 2005 from, http://blogs.zdnet.com/Ou/index.php?m=200502.

Pehkonen et a1. (2001). *Key Technologies and concepts for beyond 3G networks.* Proceeeedings of SPIE Conference-Wireless and Mobile Communications.

Phifer, L. (2003). *How can I increase the distance of coverage of WLAN?*. Retrieved June 22, 2005 from http://expertanswercenter.techtarget.com/eac/ knowledgebaseAnswer/.

Piscitello, D.M. (2002). *WLAN Security: Nipping the Problem in the Bud*. Retrieved June 14, 2005 from http://hhi.corecom.com/wsta.htm.

Potter, B., & Fleck, B. (2002). *802.11 Security*. O'Reilly & Associates.

Powers, J., & Hynes, K. (2005). *Wireless LANs. Six Steps for Enterprise & Regulatory Policy Compliance*. Retrieved May 21, 2005, from http://www.airdefense.net/.

Rappaport ,T.S. (1996). *Wireless Communications: Principles and Practice.* Retrieved March 7, 2004 from http://www.phys.unsw.edu.au/~jw/ thesis. html.

Ryan,V. (2003). "Are Wireless Networks Secure Yet?". Retrieved May 12, 2005 from http://www.newsfactor.com/perl/story/21081.html.

Secure Architectures for wireless LANs in the enterprise. Retrieved February 16, 2004, from http://www.nortelnetworks.com/solutions/security/collateral/nn101960-110802.pdf.

*Security Policies and Strategies.* (2005). Federal Information Security Conference. Retrieved June 8, 2005, from http://www.fbcinc.com/fisc/.

*Securing Wireless LANs with PEAP and Passwords.* (2004). Retrieved April 15, 2004, from http://www.microsoft.com/technet/security/topics/cryptographyetc/peap_1.mspx.

Singh, S. (1996). Quality of Service guarantees in mobile computing. Computer Communications.

*The formal WEP specification.(n.d).* Retrieved March 10, 2004, from http://standards.ieee.org/getieee802.

*The Top Seven Security Problems of 802.11*. (2003). Retrieved October 11, 2003, from AirMagnet Technical White Paper, http://www.oreillynet.com./pub/a/wireless/.

Wei-Meng, L. (2003). *An Overview of 802.11a and 802.11b Products.* Retrieved January 18, 2005, from http://www.oreillynet.com/lpt/a/3206.

*WiMAX in Action*. (n.d). Retrieved April 6, 2005, from http://www.intel.com/netcomms/technologies/wimax/.

*Wireless LAN*. (2004). SmartHome Forum. Retrieved April 21, 2005, from http://www.smarthomeforum.com./start/wlan.asp.

*Wireless Technology*. (2003). Retrieved November 8, 2003, from http://www.alliedtelesyn.com/allied/marketing/wireless/technological.htm.

*Wireless technology*. (2005). Bluetooth. Retrieved May 12, 2005, from http://www.ericsson.com/technology/tech_articles/Bluetooth.shtml

## APPENDIX APPLICATION CODES

### 1. Server Java File

```
package wlan;

import java.net.ServerSocket;
import java.io.IOException;
import java.net.Socket;
import java.net.InetAddress;
import java.io.DataOutputStream;
import java.util.Enumeration;
import java.util.Hashtable;
import java.util.Vector;

public class Server {
 protected Vector connectedUsers;
 private ServerSocket ss;
 protected Hashtable outputStreams = new Hashtable( );
 private int port;

 public Server(int port) throws IOException {
  this.port = port;
  connectedUsers = new Vector( );
  Listener a = new Listener( );
  a.start( );
 }

 Enumeration getOutputStreams( ) {
  return outputStreams.elements( );
 }

 public Object[ ] getUsers( ) {
```

```
  Object[ ] users = new String[100];
  int i = 0;
  while (outputStreams.elements( ).hasMoreElements( ))
    users[i++] = outputStreams.elements( ).nextElement( );

  return users;
}



void sendToAll(String message) {
  synchronized (outputStreams) {
    for (Enumeration e = getOutputStreams( ); e.hasMoreElements( ); ) {
      DataOutputStream dout = (DataOutputStream) e.nextElement( );
      try {
        dout.writeUTF(message);
      }
      catch (IOException ie) {
        System.out.println(ie);
      }
    }
  }
}

void removeConnection(Socket s) {
  synchronized (outputStreams) {
    System.out.println("Removing connection to " + s);
    outputStreams.remove(s);
    try {
      s.close( );
    }
    catch (IOException ioe) {
```

```
      System.out.println("Error closing " + s);
      ioe.printStackTrace( );
    }
  }
}

void checkConnections( ) {
  synchronized (outputStreams) {
    Enumeration sockets = outputStreams.keys( );
    for (Enumeration e = getOutputStreams( ); e.hasMoreElements( ); ) {
      DataOutputStream dout = (DataOutputStream) e.nextElement( );
      Socket s = (Socket) sockets.nextElement( );
      try {
        dout.writeUTF("PING");
      }
      catch (IOException ie) {
        connectedUsers.remove(s);
        outputStreams.remove(s);
      }
    }
  }
}


public static void main(String[] args) throws Exception {
  int port = 5945;
  new Server(port);
}

class Listener
    extends Thread {

  public void run() {
```

```
    try {
      ss = new ServerSocket(port);
      System.out.println("Listening on " + port);

       while (true) {
        Socket s = ss.accept();
        System.out.println("Connection from " + s);
        InetAddress serverAddress = InetAddress.getLocalHost();
        connectedUsers.addElement(s);
        DataOutputStream dout = new DataOutputStream(s.getOutputStream());
        dout.writeUTF("CONNECTED");
        outputStreams.put(s, dout);
        }
      }

    catch (IOException ioe) {
      System.out.println(ioe);
     }

   }
   }
}
```

**2. Server Application Java File**

```
package wlan;

import java.io.IOException;

public class ServerApplication {
  public static void main(String[ ] args) throws IOException {
    ServerFrame frame = new ServerFrame( );
    frame.show( );

  }

}
```

**3. Server Frame Java File**

```
package wlan;

import javax.swing.*;
import java.awt.*;
import java.awt.event.*;
import java.net.Socket;

/**
 * <p>Title: </p>
 * <p>Description: </p>
 * <p>Copyright: Copyright (c) 2005</p>
 * <p>Company: </p>
 * @author not attributable
 * @version 1.0
 */

public class ServerFrame
    extends JFrame {
  Server wirelessServer;
  JPanel panel = new JPanel( );
  String[ ] users = new String[100];
  protected JList jList1;
  JLabel connectedUserLabel = new JLabel( );
  JButton disconnectButton = new JButton( );
  JScrollPane jScrollPane1 = new JScrollPane( );
  public ServerFrame( ) {
    try {
      wirelessServer = new Server(5945);
      jbInit();
    }
```

```
  catch (Exception e) {
    e.printStackTrace( );
  }
}

private void jbInit( ) throws Exception {
  this.setTitle("Wireless Server Application");
  this.setSize(new Dimension(550, 400));
  jList1 = new JList(wirelessServer.connectedUsers.toArray( ));
  disconnectButton.addActionListener(new
      ServerFrame_disconnectButton_actionAdapter(this));
  jScrollPane1.setBounds(new Rectangle(42, 67, 457, 199));
  panel.add(connectedUserLabel, null);
  panel.add(disconnectButton, null);
  panel.add(jScrollPane1, null);
  jScrollPane1.getViewport( ).add(jList1, null);
  this.getContentPane( ).add(panel, BorderLayout.CENTER);
  panel.setBackground(Color.lightGray);
  panel.setForeground(Color.white);
  panel.setPreferredSize(new Dimension(10, 10));
  panel.setLayout(null);
  connectedUserLabel.setFont(new java.awt.Font("Dialog", 1, 13));
  connectedUserLabel.setText("Connected Users");
  connectedUserLabel.setBounds(new Rectangle(33, 45, 249, 27));
  disconnectButton.setBounds(new Rectangle(387, 275, 112, 25));
  disconnectButton.setText("Disconnect");

  Refresher r = new Refresher( );
  r.start( );
}
```

```
  void disconnectButton_actionPerformed(ActionEvent e) {
    wirelessServer.removeConnection((Socket)jList1.getSelectedValue());
    wirelessServer.checkConnections( );
  }

  class Refresher
      extends Thread {
    public void run( ) {
      while (true) {
        try {
          Refresher.sleep(5000);
          jList1.setListData(wirelessServer.connectedUsers);
          wirelessServer.checkConnections( );
        }
        catch (InterruptedException ex) {
        }
      }
    }
  }
}

class ServerFrame_disconnectButton_actionAdapter
    implements java.awt.event.ActionListener {
  ServerFrame adaptee;

  ServerFrame_disconnectButton_actionAdapter(ServerFrame adaptee) {
    this.adaptee = adaptee;
  }
  public void actionPerformed(ActionEvent e) {
    adaptee.disconnectButton_actionPerformed(e);
  }
}
```

**4. Client Java File**

```
package wlan;

import java.net.Socket;
import java.io.DataOutputStream;
import java.io.DataInputStream;
import java.io.IOException;
import javax.swing.JOptionPane;
import java.net.InetAddress;
import java.io.File;
import java.io.FileReader;
import java.io.*;


public class Client {
  private String host;
  private int port;
  private Socket socket;
  private DataOutputStream dout;
  private DataInputStream din;

  public Client(String host, int port) {
    try {
      init(host, port);
    }
    catch (Exception e) {
      e.printStackTrace( );
    }
  }
```

```
private void init(String host, int port) throws Exception {
  this.host = host;
  this.port = port;

  try {
    socket = new Socket(host, port);
    System.out.println("Connected to " + socket);

    din = new DataInputStream(socket.getInputStream( ));
    dout = new DataOutputStream(socket.getOutputStream( ));

    Runner a = new Runner( );
    a.start();
  }
  catch (IOException ioe) {
    System.out.println("Unable to connect to the wLAN");

    new Client(host, port);
  }

}

class Runner
    extends Thread {
  public void run( ) {
    try {
      int count = 0;
      while (true) {
        String message = din.readUTF();
        if (message != null) {
          if (message.equalsIgnoreCase("CONNECTED")) {
            InetAddress local = InetAddress.getLocalHost( );
```

```
          JOptionPane.showMessageDialog(null,
                                "You are now connected to the Radius Server. \nYou have been assigned the following IP Address:\n" +
                                local.getHostAddress( ));
         }
         else if (message.equalsIgnoreCase("DISCONNECTED")) {
          JOptionPane.showMessageDialog(null,
             "You are disconnected from Radius Server.");
         }
         System.out.println(message);
         break;
        }
        else {
         if (count == 0)
          System.out.println("Unable to Connect to the Wireless LAN");
         else
          ;
        }
       }
     }
     catch (IOException ioe) {
      System.out.println(ioe);
     }
   }
  }
  public static void main(String[ ] args) {

   File inputFile = new File("ClientConfiguration.txt");
   FileReader in = null;
   try {
    in = new FileReader(inputFile);
   }
```

```
    catch (FileNotFoundException ex) {
      JOptionPane.showMessageDialog(null,
                              "Unable to find client configuration file");
    }

    String host;
    BufferedReader br = new BufferedReader(in);
    try {

      host = br.readLine( );
      if (host.equalsIgnoreCase("Host_Address"))
        host = br.readLine( );
      else
        JOptionPane.showMessageDialog(null,
                              "Client Configuration File is corrupted");
      br.close( );
      in.close( );
      int port = 5945;
      new Client(host, port);
    }
    catch (IOException ex2) {
      ex2.printStackTrace( );
    }
  }
}
```

**5. Client Configuration File**

Host_Address

192.168.1.2