INTRODUCTION:

The need for networks is growing significantly and the number of Local Area Networks (LANs) in companies and institutions has increased. In the last years the technology of wireless LAN (WLAN) emerged and nowadays it reached higher levels of performance and can cover wider areas. Using this technology, a connection can be established wirelessly between different stations. Also, using some special equipment wireless LANs can be connected to wired infrastructures as well. However, one of the most challenges facing the technology is the security level compared to wired LANs. Data is sent through air and is exposed to threats form different sources. Various measurements are developed to enhance the security in these networks. In our capstone project we will first include a general overview about WLANs. We based our work on networking and communication concepts and we included a theory chapter where we explained some of the concepts that we encountered such as frame format and frequency and channel characteristics. In exploring these aspects we will have better potential to understand security threats. We also did some frequency planning and some power measurements to increase the capacity and performance of the system. Moreover, we learned different security measurements and how to implement them to our system. Through the semester we worked on our project by implementing and testing different phases and learned how they operate. In the project we used different types of devices with different features. We also created a design problem where we implemented those security measurements and illustrated how they can be used properly.

I. WIRELESS LAN OVERVIEW

The scenario of establishing a wireless connection between different stations is called a wireless LAN and they can be created using an Access Point, which is a device that serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network.

Figure1.1: Wireless LAN overview

The IEEE 802.11 also known by Wi-Fi, denotes a set of WLAN standards, which are shown in table(1.1).

Protocol	**Release Date**	**Frequency band**	**Data Rate (Max)**	**Range (Indoor)**	**Range (Outdoor)**
802.11a	1999	5-6 Ghz	54 Mb/s	30 meters	100 meters
802.11b	1999	2.4–2.5 GHz	11 Mb/s	35 meters	110 meters
802.11g	2003	2.4-2.5 GHz	54 Mb/s	35 meters	110 meters
802.11n	2006	2.4 or 5 GHz	248 Mb/s	70 meters	160 meters

Table1.1: 802.11x standards. **[3]**

Because of the easiness of deploying wireless LANs and their benefits such as mobility, the technology witnessed an enormous spread in many fields. As a result, security has become a major issue; hence various security approaches have been developed. In our project we were exposed to different security measurements and learned how to implement them as shown later.

II. THEORY

This chapter is devoted to explain two theoretical aspects of wireless LANs, which are Channels and Wireless Signals and Wireless LAN Frame Format. By gaining general ideas about these two aspects, we will be able to better understand threats to wireless LANs and methods that can be used to enhance security.

A. Channels and Wireless Signals

1) Frequency Planning:

Since the spectral width is limited, different techniques are used to manage the usage of this scarce resource. Mechanisms such as power limitation and frequency reuse were developed and deployed in Wireless LAN's. To obtain the greatest performance Access Points should not operate on the same channel simultaneously. A designer should be certain to choose the most suitable channel in a wireless network, that is, the furthest channel band from the adjacent one as shown in the Figure:

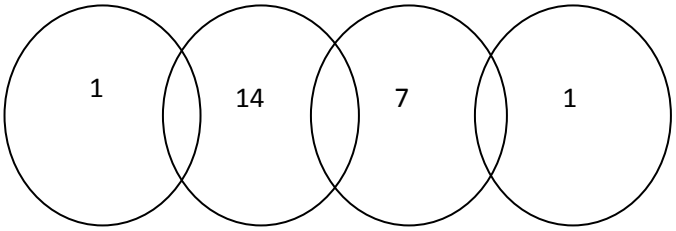

Figure 2.1: Optimize channel assignment for 802.11n

They should be set to different channels (e.g., 1, 6, and 11) in order to avoid inter-access point interference [5]. Also, some automatic channel selection features are available on the access points and can minimize the interference by assigning the least congested channels. The problem with this is automatic configuration is that sometimes roaming will not work properly and the transmission of a single access point blocks all others that are within range. As a result, performance degrades significantly[5].

Channel Identifier	Center Frequency (MHz)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

Table 2.1: Channels bands in 802.11n. [1]

2) Interference and MAC Protocol:

Using the same frequency, signals will interfere with each other and will affect the propagating signal. This interference can be avoided or minimized using CSMA\CA (Collision Sense Multiple Access with Collision Avoidance) [2,4]. The protocol is deployed in Wireless LAN's and used when two access points are using the channel simultaneously. The protocol used in Ethernet which uses collision detection cannot be used because it is difficult to detect collisions in radio environment and it is not possible to abort transmission that collides [4]. The carrier sensing involve monitoring the channel to determine whether the medium is busy or not. When the channel is busy the station will wait until the channel is unused [4]. However other stations might be waiting for the channel to be idle and the stations will transmit at the same time [4]. This can be avoided by randomizing the waiting time for each station and hence reducing the likelihood of transmitting at the same time [4].

Naturally we assumed that interference will occur when more than one signal uses the same channel simultaneously and we expected that we will not be able to establish any connection with more than one access point. However, this was not the case and we were able to establish a connection and after investigating the case we concluded that this protocol is used in wireless LAN's to avoid this type of interference.

3) Power Loss

Power transmission can be limited to the required coverage zone to allow frequency reuse and hence increase the capacity of the system. The transmitted power should take into consideration providing a Signal to Noise ratio above a certain threshold to support a reliable communication stream [3]. Electromagnetic radiation attenuates as it passes through matter resulting in decreasing signal strength. Measuring the path loss can be used to measure the power at different locations and check whether the power offers a reliable communication. An empirical formula to calculate the path loss in wireless LAN's operating on 2.4 GHz is we use

$$L(2.4GHz) = 40 + 20 \cdot \log(d) + n \cdot f + m \cdot w \text{ ,[5]}$$

Where d is the distance in meters

n and m are numbers of floors and walls between antennas and f and w are attenuation factors for floors and walls in dB.[5]

Typical attenuations through the different obstacles are presented in the following table.

Obstacle	Attenuation [dB]
Floor	30
Brick wall with window	2
Office wall	6
Metal door in office wall	6
Cinder block wall	4
Metal door in brick wall	12.4
Brick wall next to metal door	3

Table2.2: Attenuation table. **[5]**

For indoor propagation loss measurements we created the following case where three Laptops are located at different locations with respect to an access point as shown in the figure:

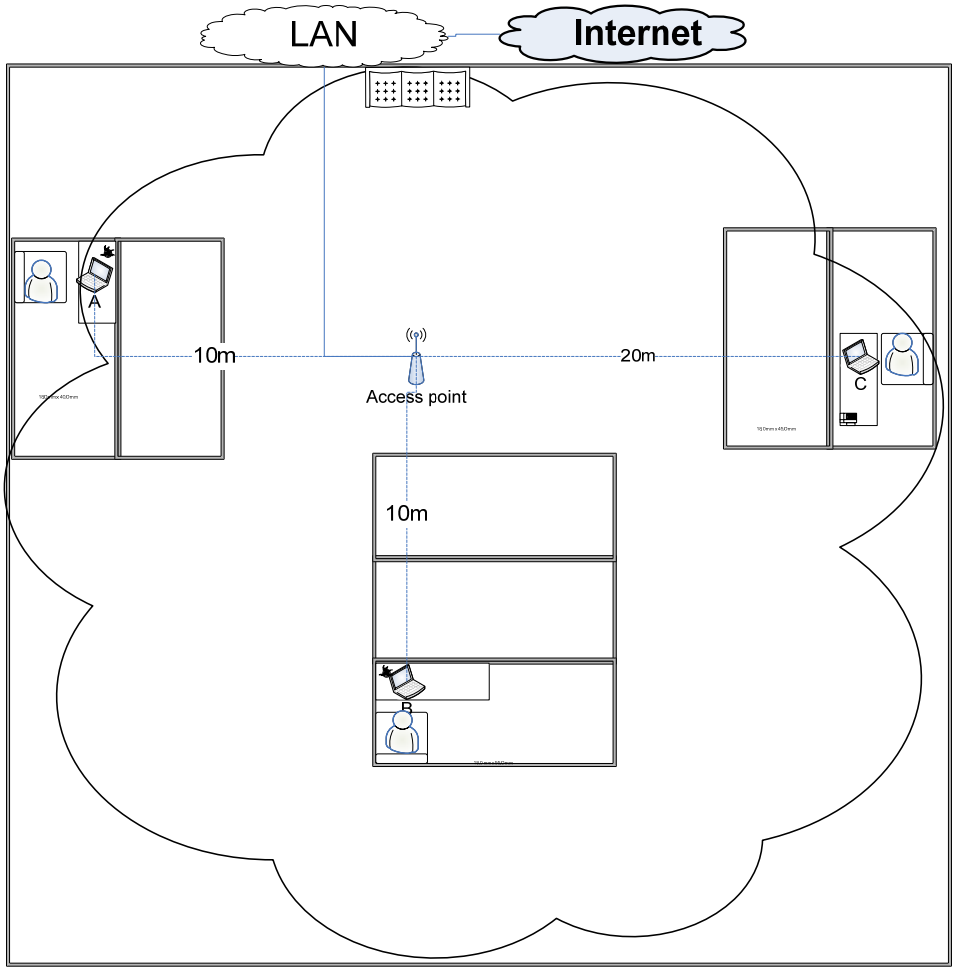

Figure2.2: Different laptops are located in different location

Station	**Distance**	Number of walls	Propagation loss (dB)
A	20	2	78
B	10	2	72
C	10	3	78

Table2.3: Propagation loss

Also power transmission can increase security measurements in the system by limiting the extent of the power to the required coverage zone. This will not allow unauthorized parties to receive the signal.

A. Wireless LANs Frame Format

Different types of frames are used by wireless LANs which involve different functions for every frame field. Each frame, field and subfield has its own role in order to run the wireless connection smoothly.

1) Basic Frame Format

Wireless LANs operate at the second layer in the OSI Reference Model, the data link layer, with each frame containing a header, a variable length body, and a trailer in the form of a 32 bit cyclic redundancy code contained in a Frame Check Sequence (FCS) field. **[3]**

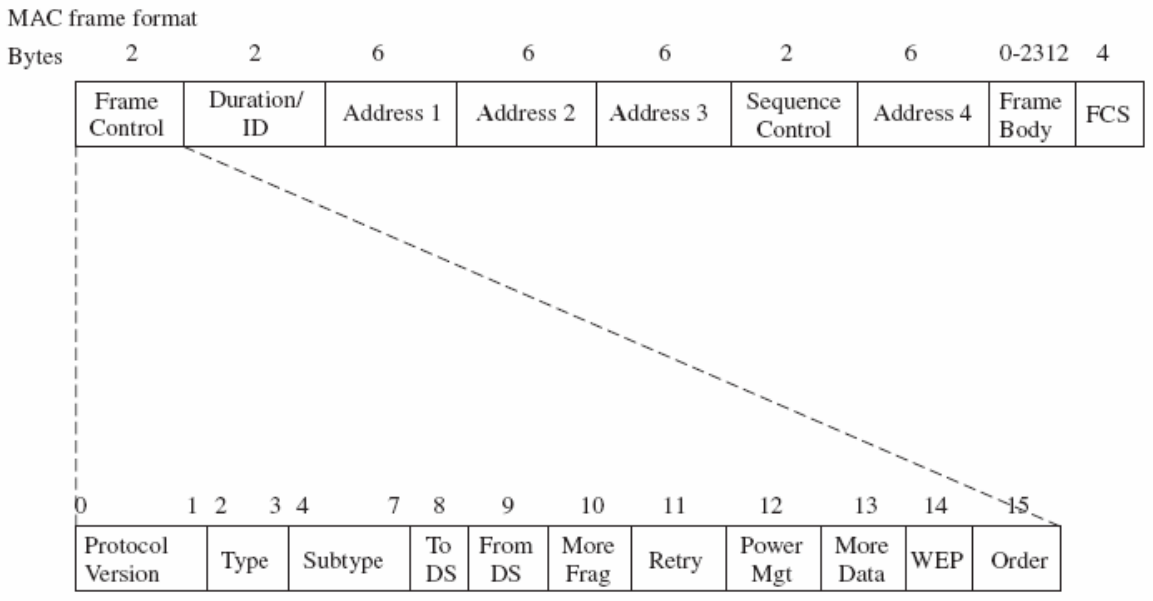

Figure 2.3: Basic wireless LAN frame format. **[3]**

- **Frame Control Field**

Each wireless LAN frame has a 16 bit frame control field which controls the information between stations and access points. The functions of its subfields are as follows:

- **Protocol Version Subfield**

It is 2 bits in length, permitting up to four versions of the protocol to be identified. The IEEE 802.11 standard commenced using a protocol version of 0, with the other values reserved for future use**. [3]**

- **Type and Subtype fields**

The Type and Subtype subfields are 2 and 4 bits in length, respectively. The value of the type frame identifies the basic type or category of a frame, while the value of the Subtype field identifies the function of the specified type of frame.

In examining the entries in Table (1.1) it is noted that presently there are three basic types of frames (management, control, data) defined, with the type field value of 11 reserved for future use.**[3]**

- **To DS Subfield**

It is 1 bit in length. The function of this field is to indicate if a data type frame is destined for a Distribution System (DS). **[3]**

- **From DS Subfield**

It is 1 bit in length. The function of this field is to indicate that a data type frame has exited from a DS. **[3]**

Type Value	Type of Frame	Subtype Value	Function
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101–1111	Reserved
01	Control	0000–1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request to Send (RTS)
01	Control	1100	Clear to Send (CTS)
01	Control	1101	Acknowledgement (ACK)
01	Control	1110	Contention Free (CF)-End
01	Control	1111	CF-End+CF-ACK
10	Data	0000	Data
10	Data	0001	Data+CF-ACK
10	Data	0010	Data+CF-Poll
10	Data	0011	Data+CF-ACK+CF-Poll
10	Data	0100	Null Function (No Data)
10	Data	0101	CF-ACK (No Data)
10	Data	0110	CF-Poll (No Data)
10	Data	0111	CF-ACK+CF-Poll (No Data)
10	Data	1000–1111	Reserved
11	Reserved	0000–1111	Reserved

Table2.4.: Relationship between type and subtype fields. **[3]**

To DS	From DS	Meaning
0	0	Data frame flows from one station to another within the same IBSS.
1	0	Data frame destined for DS.
0	1	Data frame exiting DS.
1	1	Wireless DS frame being distributed from one AP to another.

Table2.5: Relationship of To DS and From DS fields. **[3]**

- **More Fragments Subfields**

It is 1 bit in length and it is set to 1 in all data or management frames except the last frame to indicate another fragment of the frame follows. **[3]**

- **Retry Subfield**

The Retry subfield is also 1 bit in length. When set to 1 this field indicates that the frame represents a retransmission and permits a receiving station to ignore duplicate frames. **[3]**

- **Power Management Subfield**

It has a 1 bit field and it is used to indicate the power management mode of a station. A value of 1 indicates that a station is in a power save mode while a value of 0 indicates that the station is in an active mode. **[3]**

- **More Data Subfield**

The More Data subfield works in conjunction with the Power management subfield. When a station informs an access point that it is in a power save mode the AP will buffer frames for delivery to the station. When the More Data field is set to a value of 1 this indicates that at least 1 additional frame remains to be transmitted by the AP. **[3]**

- **WEP Subfield**

The WEP subfield is 1 bit in length. When set to a value of 1 this field indicates that the frame body is encrypted. **[3]**

- **Order Subfield**

It has a 1 bit field that is set to 1 in any data type frame that is being transmitted using the Strictly Ordered service class. This action prevents a change in the delivery order of frames. **[3]**

- **Duration/ID Field**

The Duration/ID field is 16 bits in length. When included in a Power Save (PS) - Poll frame this field conveys the identity of the station that transmitted the frame. In all other frames this field contains a value that indicate the number of microseconds a station requires to transmit a data frame, a control frame, or a management frame. **[3]**

- **Addresses Fields**

As shown in Figure (1.1), there are four addresses fields in a basic wireless LAN frame. The four addresses all represent 48 bit MAC addresses. The first address field conveys the destination address which indicates the final recipient of the frame. The second address field represents the source address of the station that initiated the frame. The third address is the receiver address, which identifies the intended immediate recipient of the frame, while the fourth address is the transmitter address which identifies the station that transmitted the frame. unlike a wired LAN which only has destination and source addresses, the four addresses in the basic wireless frame permits a distinction to be made between a station that originates a frame and one that transmits it over the air. **[3]**

- **Sequence Control Field**

The Sequence Control field is 16 bits in length. This field consists of two subfields, a 4 bit Fragment Number and a 12 bit Sequence Number. **[3]**

- **Frame Body Field**

As shown in Figure (1.1) you will note that the frame body can vary from 0 to 2312 bytes in length. The minimum length (0) means that there is no frame body. The maximum length results from the need of the frame body to accommodate a data unit expansion when encryption occurs. That expansion includes a 32 bit Initialization Vector (IV). **[3]**

- **FCS Field**

The last field is the Frame Check Sequence (FCS) field. This field contains a 32 bit Cyclic Redundancy Check (CRC) computed using the following polynomial:

$G(x) = x^{32} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$. **[3]**

The data is considered to represent a long binary number, which is divided by the polynomial *G(x)*. The *G(x)* value is equivalent to the binary number:

100000000110000010001110110110101

As a result of the division process the quotient is discarded and the remainder is used as the CRC. **[3]**

2) Control Frames

- **Request to Send (RTS) Frames**

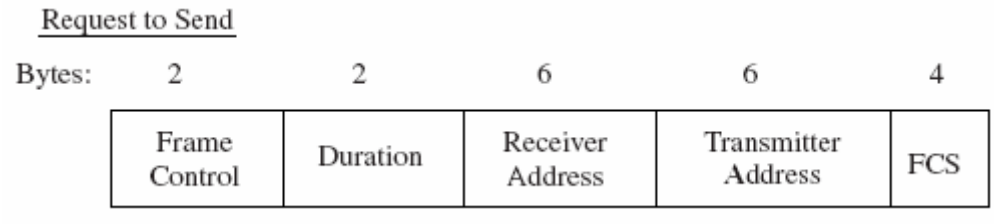

Figure 2.4: RTS frame format

When transmitting the RTS frame the station will enter a value in the duration field which denotes the length of time required to transmit its actual data frame and receive a responding ACK (acknowledgement) frame. Moreover, all stations that hear the frame are alerted to the fact that the transmitting station needs to reserve the medium for the specified period of time. Those stations then store the duration into their Net Allocation Vector (NAV), which functions as a buffer for a timer that prevent a station from transmitting whenever the NAV has a value greater than zero. The destination station will respond to the RTS with a CTS frame. **[3]**

- **Clear To Send (CTS) Frames**

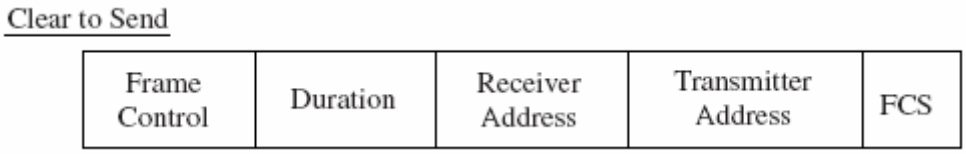

Figure 2.5: CTS frame format

Although the RTS frame caused stations to store the duration value in their NAV, those stations do not use the stored value until the receiver issues a CTS frame in response to the RTS frame. When stations hear the CTS frame, this tells them to suspend transmission for the duration defined by the RTS frame, enabling the originating station to transmit its data. **[3]**

- **Acknowledgment (ACK) Frame**

A receiving station transmits an ACK frame to the transmitting station as a mechanism to confirm the arrival of a data frame. However, instead of sending a negative acknowledgement (NAK) frame, timing is used to indicate a transmission problem. That is, instead of transmitting a NAK the receiving station does nothing. The absence of an ACK is used to indicate that the transmitted frame was either received in error or lost. **[3]**

3) Management Frames

All Management Frames are involved in a process called the Association Process, in order to better understand Management Frames; the Association Process will first be explained. **[3]**

- **The Association Process**

The initial communication between a station and an access point is called an association. The association process is accomplished through one of two types of scanning. The first type of scanning, which is referred to as passive scanning, results in a station listening to each channel for a predefined period of time .The station listens for a

special type of management frame referred to as a beacon. Access points periodically broadcast beacon frames that identify the AP and define its capabilities. Included within the beacon is an identifier referred to as a Service Set Identifier (SSID) which functions as an elementary password. Because it is possible to have multiple access points within a geographic area, stations require the ability to associate themselves with a predefined AP. To do so, you configure your station with the SSID of the access point you wish to communicate with. A second scanning method results in a station transmitting a probe frame on each channel, waiting for all access points within hearing of the probe to respond with a probe response frame. This type of scanning is referred to as active scanning. Like a beacon frame, the probe frame contains an SSID and additional information. Regardless of the type of scanning used, once a station recognizes an access point it will transmit an associate request frame. This frame will denote the capabilities of the station and the data rates it supports. The access point will respond with an associate response frame. The associate response frame includes a status code and station ID for the station. Upon receipt of the associate response frame the station becomes part of the network and can begin transmitting. **[3]**

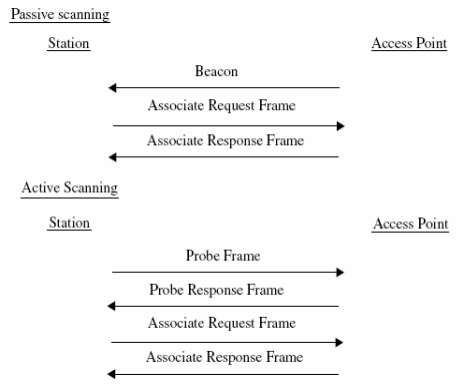

Figure2.6: Passive and active scanning

- **Beacon Frame**

A beacon frame is periodically transmitted by an Access Point to inform the stations of its presence .A timestamp, an identifier in the form of an SSID and a variety of capability information are contained in the Beacon Frame. **[3]**

- **Probe Request Frame**

A probe request frame is transmitted by a station performing active scanning during an association process. The frame also contains the SSID and the supported data rates of the station issuing the frame. **[3]**

- **Probe Response Frame**

An access point that receives a probe request frame will respond to the station issuing the frame with a probe response frame. **[3]**

- **Association Request and Response Frames**

Once a station notes the presence of an access point it can negotiate access to the AP. This negotiation process results in the transmission of an associate request frame from the station to the AP. The access point will respond with an association response frame. **[3]**

- **Disassociation Frame**

Once a station is associated with another station or access point either party can break the association. To do so the station or access point will transmit a disassociation frame which must be considered. The frame body of a disassociation frame only contains a reason code field, which indicates the reason for terminating the previously established association. **[3]**

III. WEP SECURITY ENCRYPTION

1) Background

Unlike wired cables, using the wireless medium to transmit and receive data is risky and highly unsecured. The data is easily captured by an unauthorized party since the signals are transmitted everywhere in the medium. The science of manipulating messages to secure them is called cryptography. The original message is called plaintext and the resulting encrypted message is called cipher text. The IEEE 802.11 developed the Wired Equivalent Privacy (WEP) which operates in the data link layer to encrypt the payload in individual frames **[2]**. In our senior project we used WEP configuration to encrypt the data to secure the network and in this chapter we will discuss WEP, understand how it operates and the algorithm behind it. We will also obtain an understanding of its weakness, vulnerability and how it is improved.

2) Frame Body

WEP assumes that the sender and receiver share a privet 40-bit key and a 24 bit initialization vector (IV) is generated for each frame. The IV is transmitted to the receiver since its value must be known to generate the pseudo-random sequence to decrypt the cipher text. WEP also uses an integrity check upon data since it is possible for a third party to modify the data without decrypting it. This process uses an algorithm called Cyclic Redundancy Check (CRC). This algorithm generates an Integrity Check Value (ICV) which is encrypted with the plain text. At the receiver the ICV computed from the integrity algorithm generated from the received IV and its preconfigured key is compared

with the transmitted ICV and if they are equal the integrity check is considered without error. The IV also has a 2 bit which is used to select one of four possible keys used by a station. A passphrase is a string of text used to generate the four WEP keys. **[3]**

3) Algorithm

The algorithm used for WEP is RC4 which is a variable length stream cipher that uses a key to generate an infinite pseudo-random number sequence. RC4 uses a variable length key from 1- 255 to initialize a 256 byte state table. This state table (S box array) is used to generate a pseudo-random byte stream which is XORed with the plaintext to generate the encrypted cipher text. RC4 operates on two modes key setup and ciphering. In key setup the encryption key is used with the S box array and a key array along with n swapping of bytes and modulo operations where n refers to the key's length. A key box array is also generated using the given key. For instance, if the 40 bit generated key is AB12EF54CD the key array from 1 - 255 is found by assigning K1=AB, K2=12, K3=EF, K4=54, K5=CD, and then repeating the key to fill the array, so K6=AB and so on. The encryption variables are produced by using the S and K array using some operations such as shuffling and modulo operations. Moreover a counter is used to ensure that each element is changing and another counter to change the elements randomly. Once the encryption variable is generated it is XORed with the plain text to produce the cipher or encrypted text. However the algorithm uses a small number of loops which makes it relatively fast. **[3]**

4) Weakness

As noted the IV is a 24 bit, it is transmitted in the clear part of the text and used with the secret key to generate the pseudo random sequence which is XORed with the data to produce the cipher text. A third party can easily record the transmitted data until the IV is repeated, which is known as IV collision, and XOR data with the same IV to deduce information of the contents of the two messages. We can find the duration at which the random IV repeats using the following formula **[3]**:

$$\frac{\text{Avg Frame Length}}{\text{Avg Data Transfer Rate (Mbps)}} \times \frac{8 \text{ bits}}{\text{byte}} \times 2^{24} \text{ IV combinations}$$

For example if we have a frame with 1500 bytes and a transfer rate of 11Mbps the IV will repeat every five hours as shown **[3]**:

$$\frac{1500 \text{ bytes} \times 8 \text{ bits/byte} \times 16772216}{11000000} = 18302 \text{ sec}$$

Thus using the same IV will result in the same encrypted value and using some statistical analysis to the encrypted traffic which can be used to decrypt the cipher text and hence shows that the repetition of IVs represent a weakness in WEP.

Also, an attempt to find the pseudo-random number generator and the key used to produce the sequence where an attacker can find the IP address for the packet sent and flip the address to deliver the packet to his computer in the wired network after its decrypted by the access point**[3]**.

Another weakness with the WEP can be shown if someone constructed a table for the encrypted information and by knowing some of the plaintext he can compute the RC4 generated key. The key would be then used to decrypt all the data with the same IV.

IV collision and the static key used can be encountered by using a dynamic WEP key which is referred to as WPA (Wi-Fi Protected Access). We used this modified encryption method to increase the security level of our network. TKIP (Temporal Key Integrity Protocol) is used after the initial shared secret is entered in the wireless devices and handles the encryption and automatic rekeying where the duration for which the key is changed is specified on the access point **[3]**.

IV. ACCESS CONTROL SECURITY

1) Virtual LAN (VLAN)

A) What is a VLAN

A Virtual LAN, commonly known as a VLAN, is a method of creating independent logical networks within the same network. This helps in reducing the broadcast domain and aids in network administration by separating logical segments of a LAN (like company departments) that should not exchange data using a LAN .However they still can exchange data by routing.

A VLAN consists of a network of computers that behave as if connected to the same wire even though they may actually be physically connected to different segments of a LAN. Network administrators configure VLANs through software rather than

hardware, which makes them extremely flexible. One of the biggest advantages of VLANs emerges when physically moving a computer to another location: it can stay on the same VLAN without the need for any hardware reconfiguration.

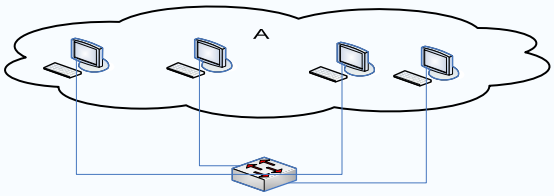

Figure4.1: Network with no VLAN

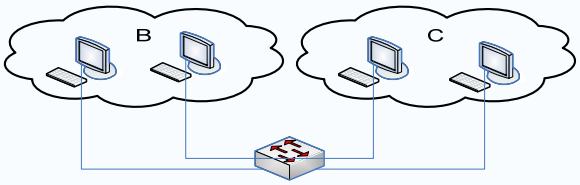

Figure4.2: Network with VLAN

As shown in the figures above networks B and C in figure: (3.2) are now different networks sharing the same switch. Another main advantage over using a router to connect two different networks connected to two different switches is getting rid of the latency created from the router that connects the LANs. It is also noticeable that VLAN produces ease in management of the networks by providing different requirements needed to each VLAN.

B) VLAN in Wireless Networks

The concept of Layer 2 wired VLANs is extended to the wireless LAN (WLAN) with wireless VLANs. As with wired LANS, wireless VLANs define broadcast domains and segregate broadcast and multicast traffic between VLANs. A unique Service Set Identifier (SSID) defines a wireless VLAN on the access point. Each SSID is mapped to a VLAN-ID.

When VLANs are not used, an IT administrator must install additional wireless LAN infrastructure to segment traffic between user groups. For example, to segment traffic between employee and guest networks, an IT administrator must install two access points at each location throughout an enterprise WLAN network (as shown in Figure:(3.3)). However, with the use of wireless VLANs, one access point can be used to provide access to all groups.

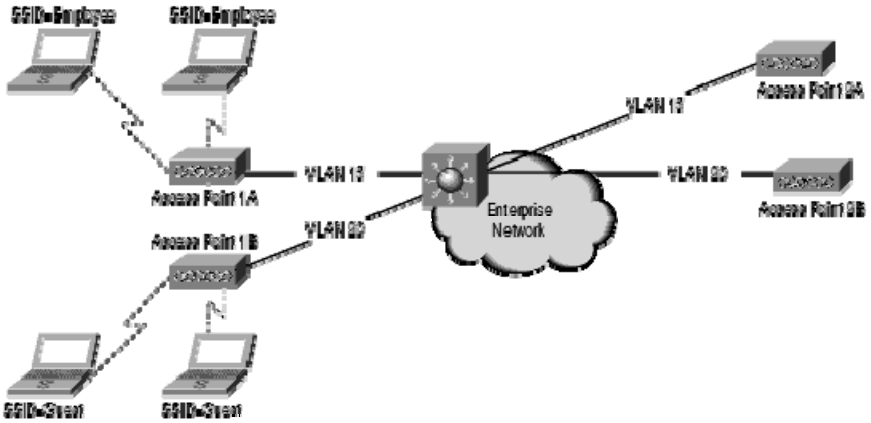

Figure4.3: Wireless connection with no VLAN

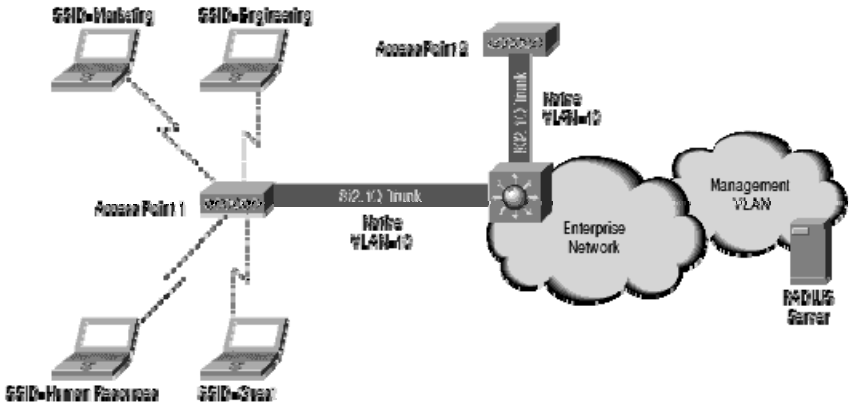

Figure4.4: Wireless connection using VLAN

Figure: (3.4) shows a company with four different departments connected to the same Access Point through the use of VLAN.

2) Filtering Based on MAC Addresses

A) What is a MAC Address

A Media Access Control Address (MAC Address) works as a unique identifier for the network adapters (NICs) and it is represented by using six groups of two hexadecimal digits, the first three groups or octants are called Organizationally Unique Identifier (OUI), since they identify the organization that issued the product .The rest of the three octants are assigned by that organization in any manner they please as long as they keep the product with a unique number

B) MAC Filtering

In computer networking, MAC filtering refers to a security access control method where the MAC Address assigned to each network card (NIC) is used to permit or prevent access to the network. The Access Points that have the MAC filtering property keep a record of the MAC Addresses saved in a list. Therefore, the administrator can freely block specific computers to access the network.

3) Network Access Control

Users in the same network can have different privileges and policies by using the Access Control option. The administrator can cease different applications by blocking their ports. Moreover, the administrator can also specify the hours in a day or days in a week to allow connection to the network.

V. EQUIPMENT

1. Cisco Aironet 1100

In our project we configured this AP which supports the IEEE 802.11g both as an access point and as a repeater The AP operates on 2.4 GHz and supports 16 SSIDs. It includes many features which increases the security level of our network. These features include:

- WEP encryption key (40 bit and 128 bit)
- WPA encryption
- VLANS
- MAC filtering
- Access restriction
- Power control

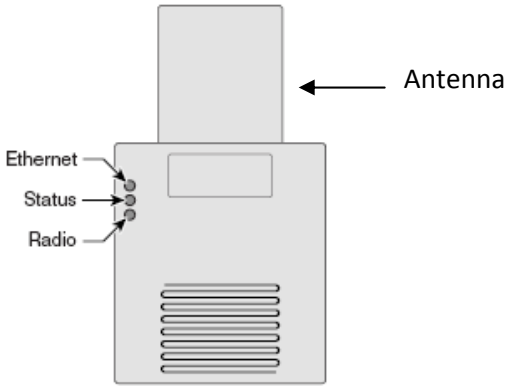

Figure5.1: Access point Layout **[1]**

LEDs

The three LEDs on the top of the access point report Ethernet activity, association status, and radio activity.

• The Ethernet LED signals Ethernet traffic on the wired LAN, or Ethernet infrastructure.

• The status LED signals operational status

• The radio LED signals wireless traffic over the radio interface. **[1]**

2. Linksys WRT300N Broad Band Route

The WRT300N was used as an access point in out project. It supports IEEE 802.11n and has a wider range (30 m indoors). It supports high bit rates 100 Mbps. It includes the following features:

MAC addresses filtering

WEP Encryption

WPA Encryption

Figure5.2: Linksys WRT300N

3. Linksys Compact Wireless-G USB adapter

This device is used to enable PCs and laptops which do not support wireless connectivity to connect to wireless networks. By incorporating USB 2.0 and Wireless-G the Adapter delivers data rates up to 54Mbps (5 times as fast as 802.11b). The Compact Wireless-G USB Adapter is also compatible with the Wireless-B (802.11b) network standard, with data rates up to 11Mbps. Also, wireless communications can be protected by industrial-strength WPA and 128-bit encryption, so data is secure.

4. Cables

We used several cables to connect between Access Points and Laptops and to connect Access Points to the Ethernet port

VI. PROJECT PHASES

Phase 1: Configuring one access point to connect to the internet

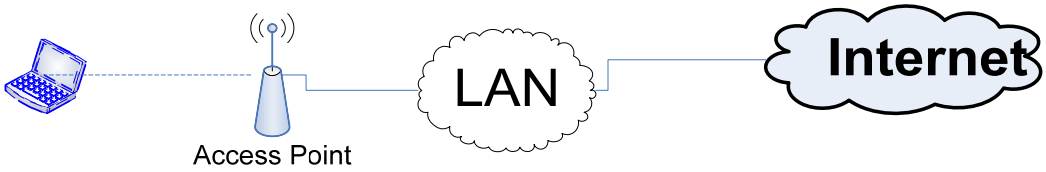

Figure6.1: One access point connected to the internet

a) Using the Aironet access point

The default IP for the Aironet access point is 10.0.0.1 with 255.255.255.224 as a subnet mask .Therefore, in order to access to the Access Point configuration menu, the computer must be in the same sub network, this is achieved by changing the IP and the subnet mask of the computer manually from the TCP/IP properties.

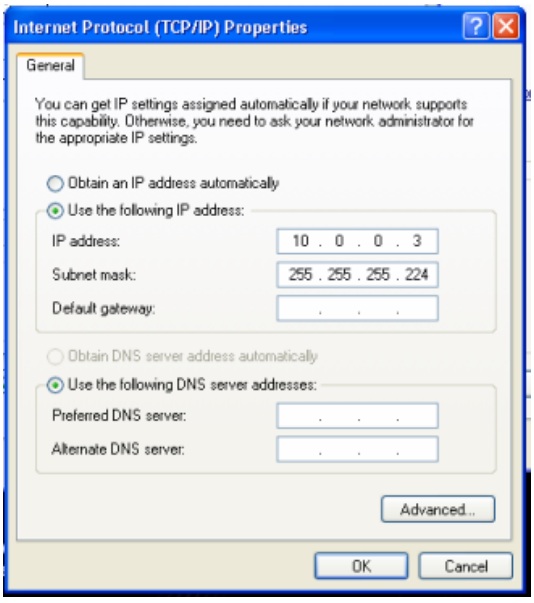

Figure6.2: Configuring the computer to access the Aironet access point

After setting the computer to access to the Access Point configuration menu, changing the Access Point's IP to 10.0.0.2 should take priority so that we can stay in the configuration menu as long as we like.

Figure6.3: Configuring the AP to 10.0.0.2

Finally, by setting the Configuration Server Protocol to DHCP , the Access point should be ready to access the internet

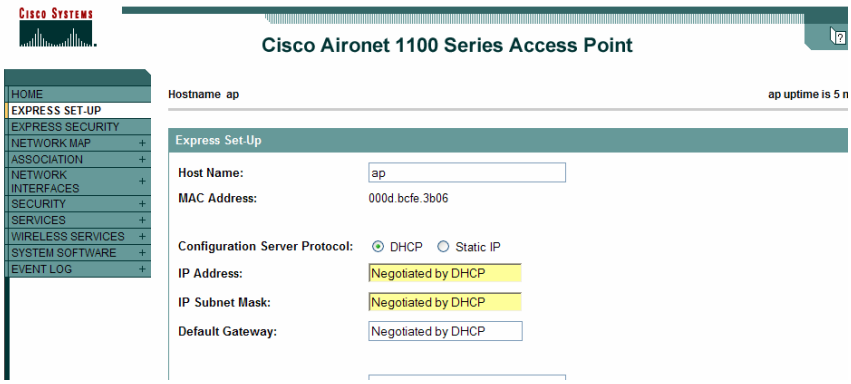

Figure6.4: Configuring the AP to DHCP

b) Using the Linksys access point

The default IP for this Router is 192.168.1.1 and it directly connects to the LAN

Phase 2: Configuring two access points one as a router and one as a repeater.

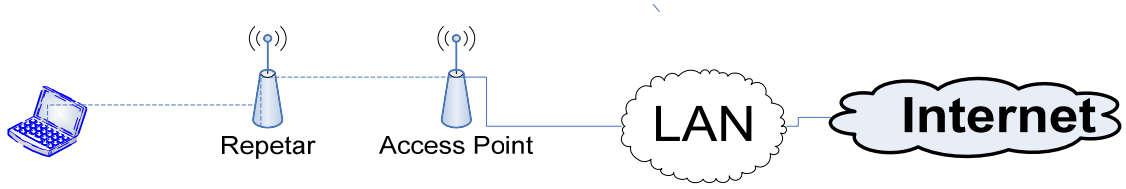

Figure6.5: A repeater connected to the access point

A repeater is a simple two-port device that amplifies the signal it receives on one port and forwards it out on the other port. To configure it, we have to match the repeater's SSID to that of the Access point's SSID and force it to work with the required Access Point. This is done from the SSID Manager under the SECURITY submenu.

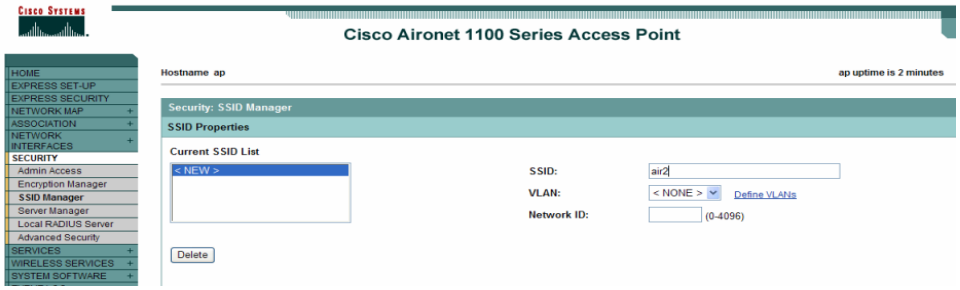

Fig6.6: Setting SSID

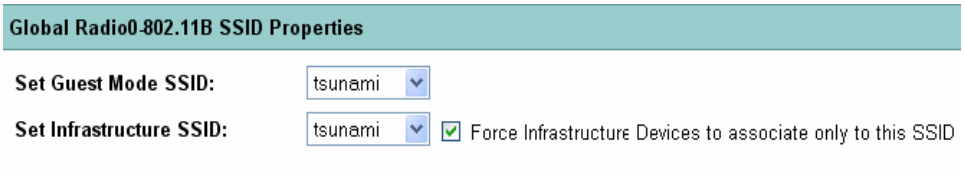

Figure6.7: Forcing the infrastructure device to associate to the SSID.\

Then, by setting repeater non-root from the EXPRESS SET-UP submenu the access point should be ready to work as a repeater.

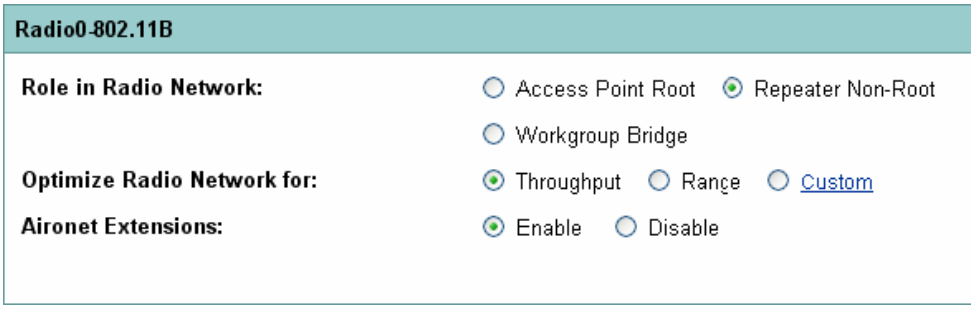

Figure6.8: Configuring the repeater

To verify that the repeater is working, we first connected the access point alone and took the LAPTOP (station) to a point where the signal could not reach. Then, we connected the repeater and found out that the station was able to connect to the Access Point.

Phase 3: Configuring two access points to work with different or same SSIDs

To configure two access point to work together its better to assign two different channels to get better performance.

Case A: two access points working as one network.

If both Access Points are assigned with the same SSID and both of them are within the range of each other. Then, one Access Point will serve as backup for the other. This was verified from the LEDs on the Aironet access point.

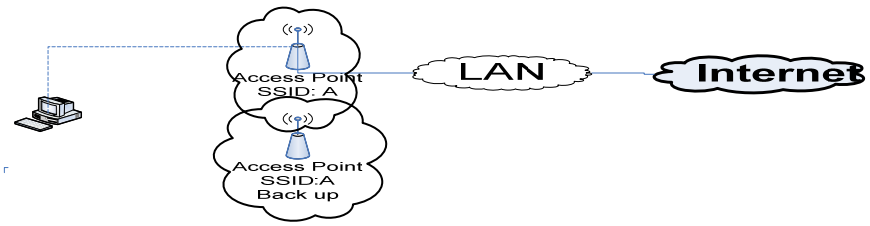

Figure6.9: Connecting to one access point with a backup access point

Case B: two access points working as two different networks.

Assigning different SSIDs to both access points will result in two different networks even if both of them are in the same range.

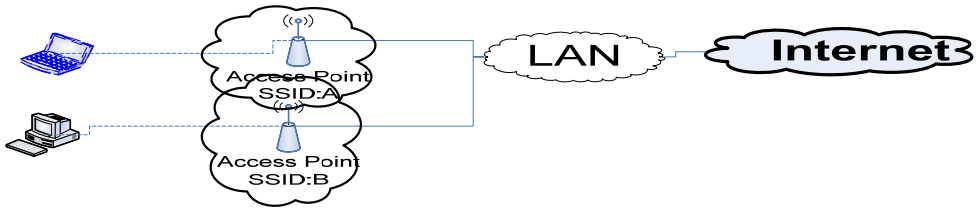

Figure6.10: Connecting two stations to two access points with different SSID's

Phase 4: Configuring two access points in two different buildings

In this phase we connected two access points in two different buildings and successfully connected one laptop from one wireless network to the other through the university's LAN. This was verified by pinging one computer using the other.

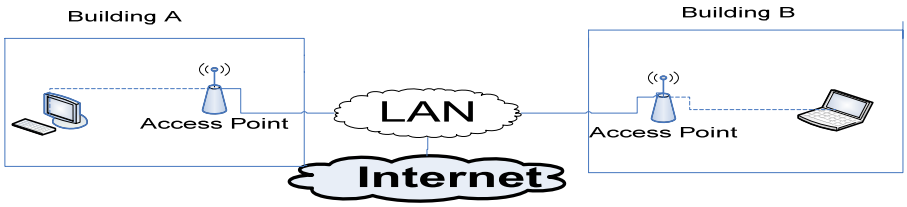

Figure6.11: Connecting two networks in two buildings

Phase 5: Configuring MAC Filtering

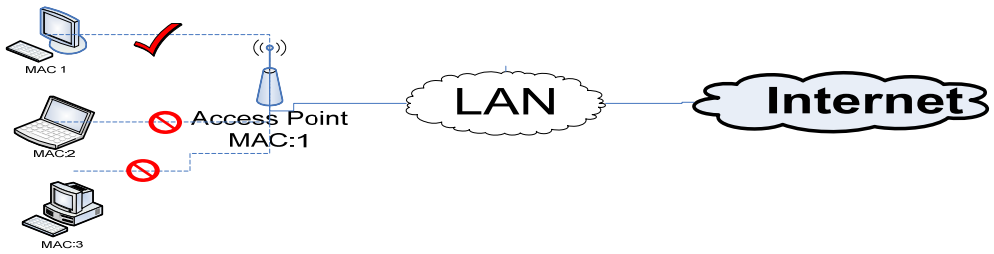

Figure6.12: MAC filtering through access points

The MAC Address of the computer can be known by entering the command (ipconfig/all) in the command prompt.

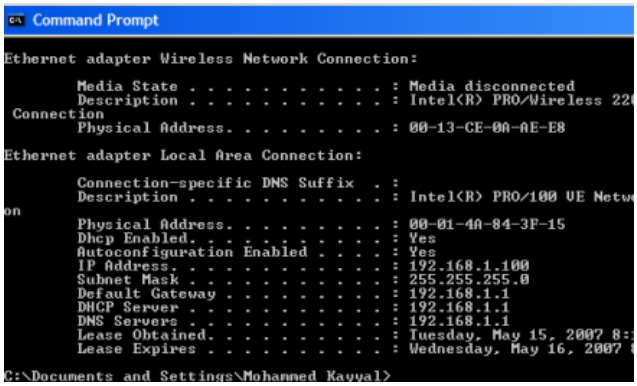

Figure6.13: Finding the MAC address using ipconfig\all

The Access Point's MAC Address filter list can be found under the MAC filtering in the Wireless submenu. By entering the MAC Addresses in the list, the corresponding computers can be allowed or denied access as shown in figure (5.14).

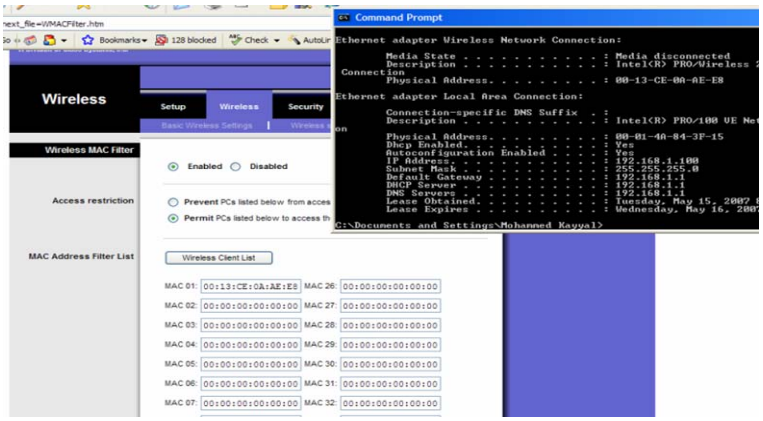

Figure6.14: Allowing only one MAC address to access through the access point

We were able to verify this by entering the MAC Address of only one laptop and chose the permit PCs labeled below option as shown in figure (5.14), by doing so, we denied access to all laptops except the one allowed beforehand.

Phase 6: Configuring WEP in Access points and stations

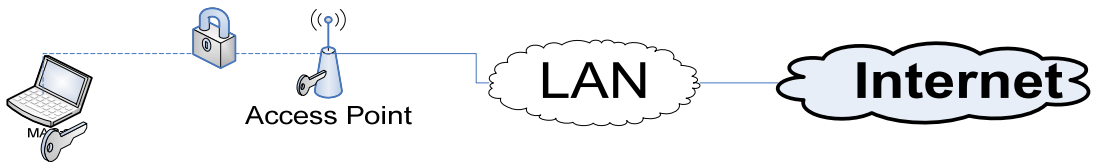

Figure6.15: Access point configured with WEP

1 - WEP configuration in Access Points

a) Using Aironet

The desired key can be entered in the static WEP key that can be found under EXPRESS SECURITY submenu, the key can either be 40 bits or 128 bits in length. Also, there are four different key numbers where only one can be used at a time as shown in figure(5.16).

Figure6.16: Configuring WEP in Aironet

b) Using Linksys

Unlike Aironet, a passphrase is entered to generate four different WEP keys with the key number instead of entering the WEP key directly and then chooses the key number. The passphrase can be entered in the wireless section under the wireless security submenu as shown in figure (5.17).

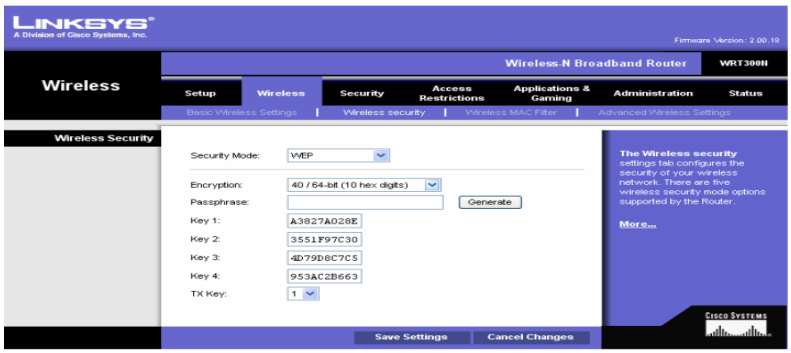

Figure6.17: Configuring WEP in Linksys

2- Stations WEP configuration

In order to implement WEP in laptops or computers, the SSIDs of the Access Points that we want to establish a connection with must be entered in the station. After that, the same WEP key and key number that were configured in the desired Access Points must be written in network key and key index respectively under wireless network properties as shown in figure (5.18).

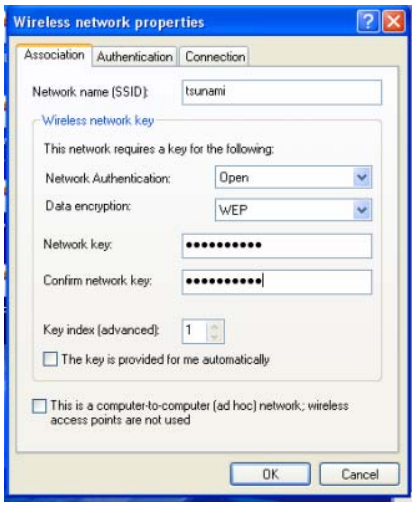

Figure6.18: Configuring WEP in PC's

Phase 7: Configuring WPA-PSK in Access Points and stations

WPA Configuration in Access Points

As mentioned, WPA-PSK is an evolved encryption method where the key changes periodically using the TKIP. To configure it, we set the security mode to PSK-Personal and choose TKIP in the encryption slot with the desired key renewal period. This is also found under wireless security submenu.

Figure6.19: Configuring WPA in Linksys

WPA-PSK Configuration in Stations

Just like WEP. However, WPA-PSK network authentication and TKIP data encryption are used instead of WEP. Then, the network key in entered with no key indexes used.

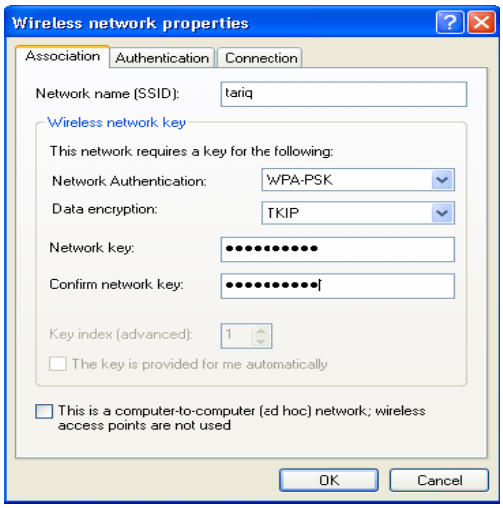

Figure6.20: Configuring WPA in PC's

We successfully verified the WEP AND WPA-PSK encryption methods as shown in figure (5.21), the upper one (air1b) is secured with WEP and lower one (link1) is secured using WPA.

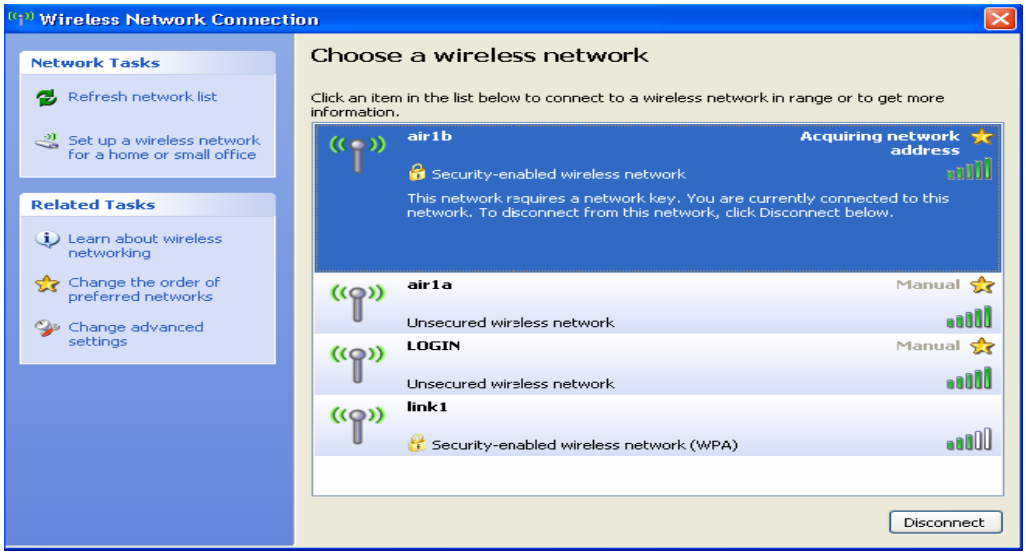

Figure6.21 air1b configures as a VLAN and link 1with WPA

Phase 8: Configuring Network Access Control

Figure6.22: Access restriction with HTTP blocked

As mentioned, this method allows the denial of specific applications according to the administrator wishes, where different ports can be blocked and allowed to provide different privileges to the network's users. Figure (5.23) shows how a port can be blocked. This can be done by entering the Access Restrictions submenu.

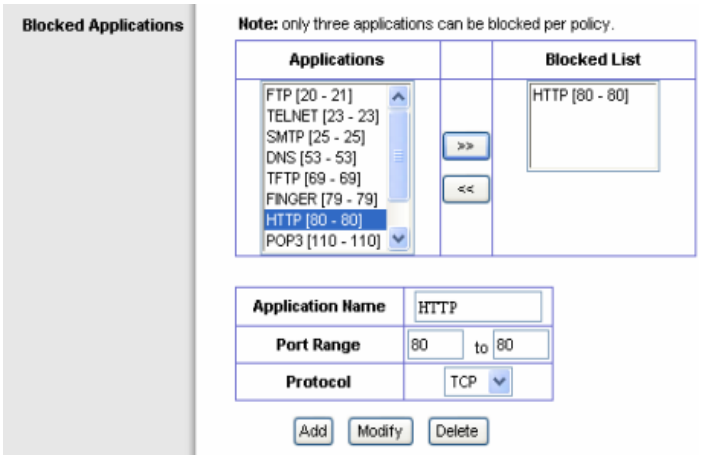

Figure6.23: Blocking HTTP port

Phase 9:Configuring VLAN

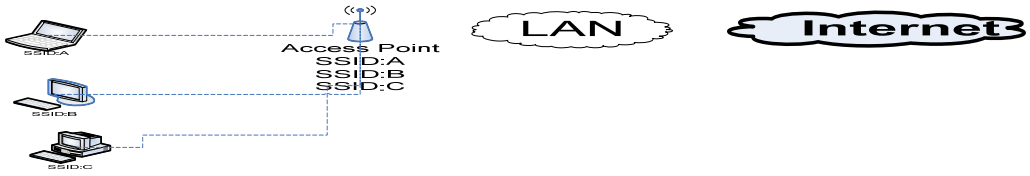

Figure6.24: Configuring VLANs

To configure VLANs, several SSIDs must be created within the same Access Point. Then each SSID should be mapped to a VLAN-ID. This can be done from the EXPRESS SECURITY submenu as shown below.

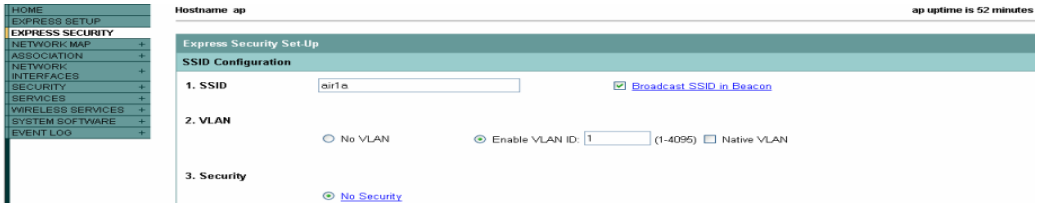

Figure6.25: Enabling VLANs

Since only one SSID can be broadcasted, it is essential to enter the SSID of the desired VLAN in the station's wireless network properties.

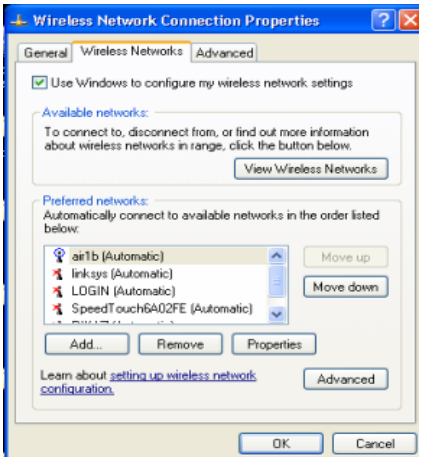

Figure6.26: Configuring VLANs on PCs

VII. DESIGN EXAMPLE

There is a company with two different buildings, building (A) is shared between normal employees and guests and building (B) is for the manager and it has a meeting room shared between employees. Also, let us say that there is a parking lot for the company near building (A) and another wireless LAN in a coffee shop just outside the company's boundaries located near building (B) as shown in the figure below.

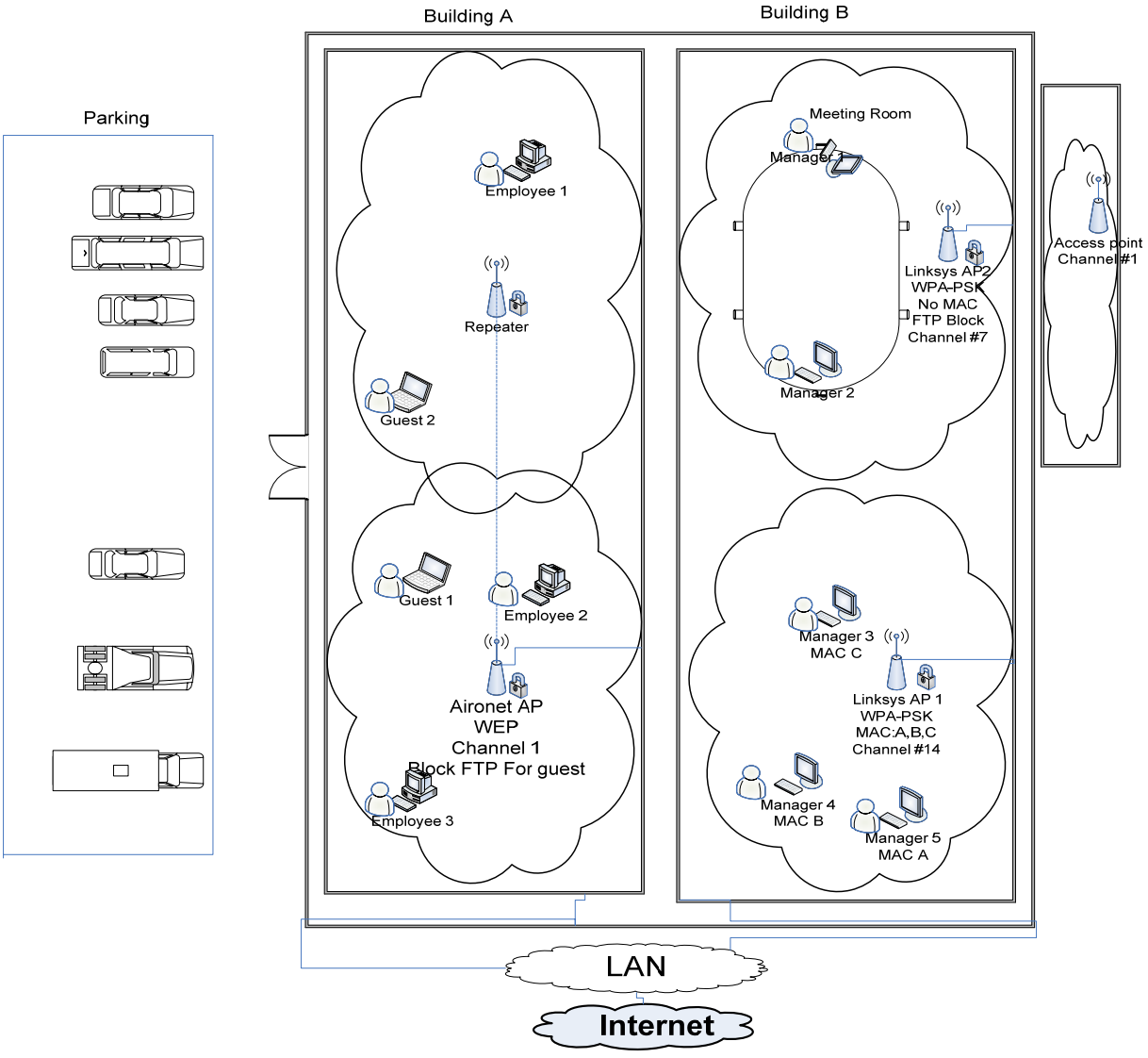

Figure 7.1: Design illustration

Building (A) was configured as follows:

- Configured with two Aironet APs, one of them works as a repeater to enhance the coverage of the network to cover the whole floor in building (A).
- Power management was considered so that the network coverage does not exceed the building's boundaries and insure that the network does not reach the parking lot where a lot of unauthorized people might have access to.
- Since both normal employees and gusts have different privileges, VLANs were configured to separate between their networks.
- The FTP port was blocked in the gusts VLAN so that the bandwidth would not be consumed by them.
- WEP with 40 bits encryption key was configured to the guests VLAN and with 128 bits encryption key was configured to the normal employees VLAN. Since Building (A) has a high traffic due to high number of users, WEP was chosen considering that the encryption is relatively fast and easier to implement compared to WPA. Whereas 128 bits is used to increase the level of security to normal employees.
- Channel (1) was assigned to building (A)'s network to avoid interference with building (B)'s network where channels (7) and (14) were assigned there.

Building (B) was configured as the following:

- Two Linksys APs were configured in building (B), AP (1) for the managers and AP (2) for the meeting room.
- AP (1) was configured with MAC filtering to allow only the managers computers to enter the network.
- AP (2) was not configured with MAC filtering since it is deployed in the meeting room where any employee can enter. However, FTP port was blocked to save the bandwidth.
- Both AP (1) and (2) were configured with WPA-PSK seeing that managers require more security because they have more critical information. Moreover , network speed will not be an issue since there are less number of users in building (B)
- Channels (7) and (14) were assigned to AP (2) and AP (1) respectively. This is done to avoid interference with the coffee shop and building (A) since both of them use channel (1).

CONCLUSION:

During the capstone project we were exposed to security which is a fundamental element of networking. We successfully implemented a satisfactory amount of security parameters which increased the security level in our designed network. We also enhanced our concepts and developed some theories in fields such as encryption and frame format and we applied some IP and subneting concepts to configure the Aironet access points. Moreover, we verified some of the protocols used in WLAN's and their effect, for example CDMA\CA would allow two AP's to work simultaneously on the same channel. We also adjusted power transmission to limit the channel interference and to increase the security level.

Also, we worked effectively as a group, where we shared different phases and consulted each other when facing problems. We also discussed our concerns and problems with our supervisors and we met regularly to discuss our progress and future plans.

In the project we faced many problems and we spent a lot of time to investigate and to resolve them. For example in access restriction even though we blocked some ports, users were still able to access these ports. We contacted Linksys technical support and we have been told to update the firmware (software) of the access point.

This project can be implemented in different scenarios where the security aspects can be implemented depending on the case and the level of security needed.

In the future, this project can be assigned to another group of students where they can use some tools to implement some threats on the network and work on blocking these

threats. They can also use some sniffing tools to observe the encrypted and decrypted frames and investigate other encryption algorithms.