

Security Design for Wireless Local Area Network (WLAN)

By

Feizol bin Ahmad

Project Dissertation submitted in partial fulfillment of
the requirements for the
Bachelor of Technology (Hons)
(Information Technology)

JUNE 2004

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

*

TK

5103.2

F297

2004

1) Wireless Communication Systems

2) IT/IS - Thesis

CERTIFICATION OF APPROVAL

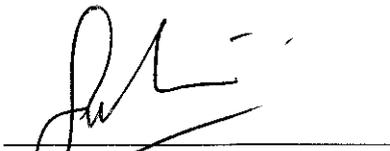
Security Design for Wireless Local Area Network (WLAN)

by

Feizol Bin Ahmad

A project dissertation submitted to the
Information Technology Programme
Universiti Teknologi PETRONAS
in partial fulfillment of the requirement for the
BACHELOR OF TECHNOLOGY (Hons)
(INFORMATION TECHNOLOGY)

Approved by,



(Mr. Suhaimi Abdul Rahman)

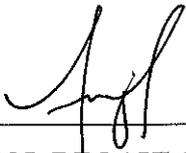
UNIVERSITI TEKNOLOGI PETRONAS

TRONOH, PERAK

June 2004

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.



FEIZOL BIN AHMAD

ABSTRACT

Wireless networking is rising with the ever-increasing need for businesses to lower costs and support mobility of workers. Compared with wired networking, wireless capability offers more timeliness, affordability, and efficiency. When performing installations, there are many tangible cost savings with using less wire between the user's appliance and a server. However, most of the organization that decided to deploy wireless network within their working environment often overlooked the security aspect of the deployed wireless LAN. Therefore, this will jeopardize the organization's safety in terms of network security and business trade secrets if their network is intruded by their rivals. This project concentrates on Wireless Local Area Network architecture and the security aspect of the designed network. Firstly, the project will emphasize on researching about WLAN architecture. This is to ensure best practice method to be taken in designing the WLAN. It is then followed by extensive research to deploy better security to the designed network. However, the security aspect to be deployed is based on the needs and the architecture of the WLAN. The designed network is tested by conducting similar simulation at the lab which represents real - time performance and situation where the network architecture will be implemented and tested. For the time being, 802.1X / EAP (Extensible Authentication Protocol) is proven to be the best practice solution to secure any Wireless LAN implemented. Through the simulation, it will be proven that the proposed WLAN design is secure for implementation by any other interested parties.

ACKNOWLEDGEMENT

Alhamdulillah, this project has finally come to an end. First of all, I would like to thank Universiti Teknologi PETRONAS for giving me the opportunity to complete my final year project here.

I would like to thank Mr. Suhaimi Abdul Rahman, my final year project supervisor in Universiti Teknologi PETRONAS for assisting me with his inspirational contributions throughout the early stages of this project until the end. His advice and suggestions have been very helpful in order for me to carry out the project work. My gratitude goes to all the Information Technology and Information Systems lecturers that have either helped me directly or indirectly in order to successfully complete this project.

Special thanks go to Mr. Ruslan of Data Communication Lab of Universiti Teknologi PETRONAS for his great contribution in providing useful information and preparation on the equipments needed for my final year project.

My sincere thanks also go to my parents who understand the difficulties and are always there for me. Thanks also go my colleagues; especially my laboratories colleagues that have shared the same experience of making each individual final year project a success.

Last but not least, I would like to thank those who have helped me and supported me directly or indirectly to the outcome of this project. I would not have been able to complete this project without your help.

TABLE OF CONTENTS

| | | |
|------------------------|---------------------------------------|----|
| ABSTRACT | | i |
| ACKNOWLEDGEMENT | | ii |
| CHAPTER 1: | INTRODUCTION | 1 |
| | 1.1 Background study | 1 |
| | 1.2 Problem statement | 2 |
| | 1.3 Objectives and scope of study. | 2 |
| | 1.3.1 Relevancy of the project | 2 |
| | 1.3.2 Objectives of the project | 3 |
| | 1.3.3 Scope of study | 3 |
| | 1.3.4 Feasibility of the project | 3 |
| CHAPTER 2: | LITERATURE REVIEW AND THEORY | 4 |
| | 2.1.1 Wireless Technology | 4 |
| | 2.1.2 Security | 6 |
| CHAPTER 3: | PROJECT WORK | 10 |
| | 3.1 Project Work | |
| | 3.1.1 Project Analysis | |
| | 3.1.1a Hardware Requirement. | 11 |
| | 3.1.1b Software Requirement. | 11 |
| | 3.2.1 Project Design | |
| | 3.2.1a IPSec | 12 |
| | 3.2.1b 802.1X / EAP | 13 |
| CHAPTER 4: | RESULTS AND DISCUSSION | 20 |
| CHAPTER 5: | CONCLUSION AND RECOMMENDATION. | 27 |
| REFERENCES | | 30 |

List of Figures

| | |
|--|----|
| Figure 2 – A : Encrypted WEP framed | 7 |
| Figure 3 – A : IEEE 802.1X Setup | 14 |
| Figure 3 – B : Suggested design of wireless LAN using 802.1X / EAP | 17 |
| Figure 3 – C : Enabling Authentication on Cisco Aironet Access Points | 18 |
| Figure 3 – D : Identifying the local RADIUS Server | 19 |
| Figure 4 – A : Test environment for 802.1X / EAP Solution | 20 |
| Figure 4 – B : Creating User Account on the RADIUS Server | 21 |
| Figure 4 - C : Setting Up User Access Permission | 22 |
| Figure 4 – D : Setting Up Certification Authority | 23 |
| Figure 4 – E : Changing the Security Setting of the connection | 23 |
| Figure 4 – F : Successful reconnected using 802.1X / EAP protocol using a Cisco 350 AP series | 24 |

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND STUDY

The wireless LAN is normally deployed is developed by the IEEE and regulated in Europe is 802.11b which is also referred to as Wi-Fi. 802.11b provides for data speeds of 11Mbps using the 2.4GHz band. By having an access point that plays the same role as central hub / switch in wired networks, Wireless LAN is able to replace wired Ethernet technology for better productivity.

This project is aimed to develop a secure, reliable Wireless Local Area Network (WLAN) setup and implementation by extensive research of WLAN designing and architecture. Since nowadays many company and firms chose to adopt wireless network to increase mobility and flexibility between employees, some of them are exposed to potential attack and loophole.

To ensure security and reliability of the networks, all design and configuration are based on researched guideline and blueprints. Therefore, the outcome of this research will able to provide best practice information and virtual-private-network in both configuration and topologies.

1.2 Problem Statement

As for the time being, Wireless LAN or WLAN rapidly became popular within the community. Many ISP and technology firm started implementing WLAN for higher mobility and accessibility to their own networks for better productivity. However, in certain cases, WLANs are designed just to meet the user requirements and often overlooked the security elements of the WLAN. Most implementations are done with the basic design for security, only relying on Wired Equivalent Privacy (WEP) protocol that is used to protect link-layer communications from eavesdropping and other attacks, which bearing high potential for exploitation and flaws. This could lead to jeopardizing business secret for big firms that implemented WLAN within their organization and could create a substantial loss. This project is going to look at one definite architecture and configurations that can be implemented on a newly installed wireless network. With extra emphasize of protecting user networks, rather than providing wireless networks the proposed and recommended design will result a secured networks.

1.3 Objective and Scope of Study

1.3.1 The Relevancy of the Project

There are two different criteria involved in each stage of the development process.

- *Research on the wireless LAN.*

Research will be carried out on how Wireless Local Area Network going to be designed and implemented.

- *Securing the WLAN design and architecture.*

Upon identifying and designing the recommended wireless LAN, works to secure each WLAN is going to be carried out to meet the requirement and objectives.

1.3.2 Objective(s)

This project is aimed to :

- Develop a working WLAN architecture with maximum security, by implementing approaches that could prevent any potential weaknesses and loopholes that could be exploited by outsiders.
- Develop a simulation / guide to help users to configure their WLAN based on designed framework.

1.3.3 Scope of study

- The scope of this project will concentrate on researching the best method and design to protect one implemented wireless design.
- The study also will include how we can utilize the pre-defined WEP encryption to minimize any potential threat and intrusions to the network.

1.3.4 Feasibility of the Project within the Scope and Time Frame

- This project relies heavily in researching and understanding skills of the author, therefore most of the time spent is used to gather as much information and usable literature to help with designing the framework.
- By quickly understanding and able to adopt the theories gained through extensive reading of literature material, it is feasible to complete the project.

CHAPTER 2

Literature Review and Theory

2.1 Literature Review and Theory

2.1.1 Wireless Technology

According to (<http://www.whatfs.com>),

The term wireless refers to telecommunication technology, in which radio waves, infrared waves and microwaves, instead of cables or wires, are used to carry a signal to connect communication devices. These devices include pagers, cell phones, portable PCs, computer networks, location devices, satellite systems and handheld digital assistants.

There is a wide-range of wireless devices that implement radio frequency (RF) to carry the communication signal. Some wireless systems operate at infrared frequencies, whose electromagnetic wavelengths are shorter than those of RF fields. Wireless systems can be divided into fixed, portable, and Infra Red (IR) wireless systems.

A fixed wireless system uses radio frequencies requiring a line of sight for connection. Unlike cellular and other mobile wireless systems, they use fixed antennas with narrowly focused beams. Fixed wireless systems can be used for almost anything that a cable is used for, such as high-speed internet connection, and satellite television connection. Technology has brought higher radio frequencies with broader bandwidth that can carry

more information, and require smaller antennas, resulting in lower costs and easier to deploy systems.(Peter Rysavy, 2003)

A portable wireless system is a device or system, usually battery-powered that is used outside the office, home, or vehicle. Examples include handheld cellular phones, portable computers, paging devices, and personal digital assistants (PDAs), which operate through microwaves and radio waves.

An IR wireless system uses infrared radiation to send signals within a limited-range of communication. These systems are commonly used in television remote-control boxes, motion detectors, and cordless computer keyboards and mice. With progressing new technologies, IR wireless systems can now connect notebook computers and desktop computers used within the same local area network (LAN) workstation, which will heavily impact the way we conduct meetings, presentations, and daily business, at the office.

One of the benefit by using WLAN was mentioned by Tiho Vukasinovic

“I live in an old house and I'm planning a home renovation project. When my stock options have nested long enough I'll tear down the inner walls and rebuild the place from scratch, throwing in some CAT5e cabling while I'm at it. In the meantime I've had to find a way to link my computers together and share my Internet connection without drilling holes or carving walls. Furthermore, I've wanted to be able to roam around the house, taking my portable out on the terrace to enjoy the little sunshine we get in our country.”

Vukasinovic later found out more benefit from WLAN and did not use CAT5 cables at all, after doing some calculation and cost realization of WLAN implementation and compared it with wired LAN before kept on using WLAN.

The wireless LAN is normally deployed is developed by the IEEE and regulated in Europe is 802.11b which is also referred to as Wi-Fi. 802.11b provides for data speeds of 11Mbps using the 2.4GHz band.

2.1.2 Security

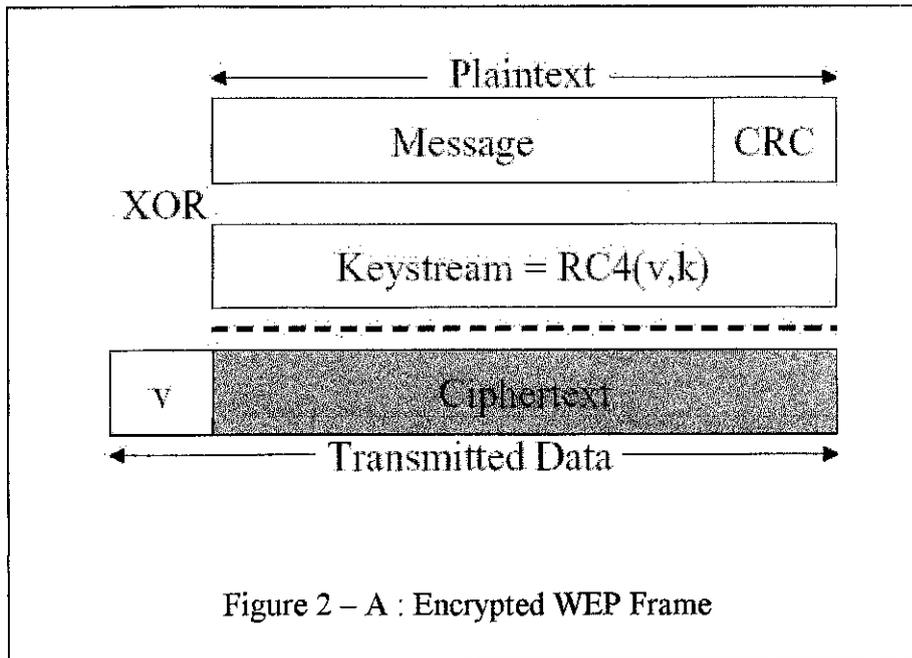
Refers to the safety of an organization, person or a group of people from unwanted things. In networking terms, security can be defined as the safety of one network from unwanted traffics, entity (things) that could result to a disaster.

It is crucial when designing a network; implementing the security aspect of the network is the most difficult part of the plan. Considering technology changes day by day, more bug, flaws and exploit are found in existing technology and gadgets.

When discussing 802.1X, it is known that the main security aspect of this architecture is the embedded Wired Equivalency Privacy (WEP). The 802.11 standards define WEP as a simple mechanism to protect the over-the-air transmission between WLAN access points and network interface cards (NICs). Working at the data link layer, WEP requires that all communicating parties share the same secret key. To avoid conflicting with U.S. export controls that were in effect at the time the standard was developed, 40-bit encryption keys were required by IEEE 802.11b, though many vendors now support the optional 128-bit standard. WEP can be easily cracked in both 40- and 128-bit variants by using off-the-shelf tools readily available on the Internet. On a busy network, 128-bit static WEP keys can be obtained in as little as 15 minutes, according to current estimates.

WEP uses the RC4 stream cipher that was invented by Ron Rivest of RSA Data Security, Inc. (RSADSI) for encryption. The RC4 encryption algorithm is a symmetric stream cipher that supports a variable-length key (refer Figure 2 – A). The IEEE 802.11 standard describes the use of the RC4 algorithm and key in WEP, but does not specify

specific methods for key distribution. Without an automated method for key distribution, any encryption protocol will have implementation problems because of the potential for human error in key input, escrow, and management. As discussed later in this document, 802.1X has been ratified in the IEEE and is being embraced by the WLAN vendor community as a potential solution for this key distribution problem.



Recent findings by cryptanalysts, Fluhrer, Shamir and Mantin shows that RC4 algorithm used on deployed WEP which a fixed secret key is concatenated with known modifiers in order to decrypt messages. After an attacker successfully grabbed bits of the encrypted transmitted data, it would be easy to decrypt the data using available tools on the internet.

Many research and discussion has been conducted to overcome the weaknesses of WEP that is mainly used by firms that adopted WLAN within the organization environment. However, relying too much on WEP alone would compromise the organization's security if there is third party that interested in breaking into the organization's network. This several serious security flaws had been found in WEP, which can lead to rise of number of attacks on WLAN. (Borisov, Wagner 2001)

Mishra and Arbaugh (2003) is very definite, "Users are adopting the technology to save the time, cost and mess of running wires in providing high speed network access. Hot spot areas such as airports and coffee houses are embracing the technology to provide additional value to their customers with the hopes of increasing their revenue. One of the main reasons organization are quickly adopting 802.1X based security is that the current security problems with wireless local area networking based on the IEEE 802.11 standard are well known and IEEE standard Task Group on Security (TGi) have been working on solving the problem for some time." Even with the flawed security protection, most organization sees increase in revenue is far better than having their secret exposed to interested parties who are able to exploit the available WLAN. Hence, making the reason why organization needs to start deploying strategies to protect their WLANs rather than bearing more losses in terms of business advantage.

Tiho Vukasinovic realized that the Wired Equivalent Privacy (WEP) security mechanism in IEEE 802.11b defines a secret key encryption method to make data in the air unreadable for outsiders, but it does not define how the secret keys are to be distributed to the client and to the Access Point nodes. In practice, the secret key will either be stored on the network card or entered manually by a user or administrator on the systems in a wireless workgroup. This is very inconvenient and carries a huge security risk since keys are easily exposed and often remain unchanged due to the effort it takes to change them.

According to 802.11 standards, WEP acts as a simple mechanism to protect the over-the-air transmission between WLAN access points and network interface cards. This requires all communicating party to share the same secret key, usually 40-bit encryption keys. However, on a busy network, 128-bit static WEP can be obtained in 15 minutes, using off-the-shelf tools by gathering as low as 1 million packets before being able to crack the key within seconds. (Convery, Miller 2003).

The 802.1X standard is intended to provide strong authentication, access control and key management. Unfortunately, initial analysis of the protocol when used in conjunction with WLAN 802.11 standards shows that the protocol fails to provide strong access control and authentication, after series of test by Mishra and Arbaugh(2003).

Although traditional WLAN security that relies on open or shared keys and static WEP keys, it is better than no security at all but it is not sufficient for the enterprise organization. Only very small businesses, or those that do not entrust mission-critical data to their WLAN networks, can rely on these WLAN security types. All other enterprises and organizations must invest in a robust, enterprise-class WLAN security solution.

CHAPTER 3

PROJECT WORK

3.1 Project work

In order to design a secure and reliable WLAN framework, this project will rely heavily on researched white paper and tutorials provided by leading network consultant firms. Therefore, prototype model can be applied here by designing a prototype product for review and evaluation for further enhancement.

The project started off with,

- Intensive research and data mining of available framework and design,
- With the theories acquired, prototype based on the framework is built.
- However, limited technical capability and knowledge in WLAN framework requires ongoing discussion and peer review of the different module to ensure usability and compliant to requirement and scope.
- The finalized framework would be presented in series of simulation and also being proven in real time testing which would be decided later.
- The usage of simulation and demonstration to give extra information and comprehension to interested party on how does the designed network ensures the reliability and security of the organization.

3.1.1 Project Analysis

In order to start developing a network, it is crucial to analyze current situation, needs and requirements for more in-depth and understanding to prevent any mistakes or flaws during design phase.

One of the important criteria need to be considered is the need of wireless network. For a small, new company, it is understandable for them to deploy a wireless LAN for lower cost compared to installing cables and network ports. For large sized company or firm, going wireless meaning they are intending to expand their staff mobility and to increase production.

It also important to analyze requirements for each scale of network intended to be design, either hardware and software requirement.

3.1.1.1 Hardware Requirement

Basically, for every WLAN implementation, the equipment needed will be more or likely the same

- Access Point (AP) or wireless bridge
- A server to perform as a domain controller, a Domain Name System (DNS) server, a Dynamic Host Configuration Protocol (DHCP) server, and a certification authority (CA).
- A server to act as a Remote Authentication Dial-in User Service (RADIUS) server.
- Personal computer with Wireless 802.1x compatible card installed.
- Connection to outside network

3.1.1.1 Software Requirement

For the time being, the simulation and testing is intended to be done on Microsoft Windows platform, therefore

- DNS server, DHCP , Radius server will be using Microsoft Windows Server 2003 with Service Pack 4
- Clients will be using Microsoft Windows XP Professional

3.2.1 Project Design

As we are emphasizing security aspect in the intended network design, therefore, we will need to select the best practice method to be implemented in the network. Considering the many option we have, it is decided that we need to analyze each and every solution we have in our hand

3.2.1.1 Solution 1 : Wireless Network with IPsec

IPsec is an acronym for Internet Protocol Security. A security protocol from the IETF (Internet Engineering Task Force) that provides authentication and encryption over the Internet. Unlike Secure Sockets Layer, which provides services at layer 4 and secures two applications, IPsec works at layer 3 and secures everything in the network.

Since IPsec was designed for the IP protocol, it has wide industry support and is expected to eventually become the standard for VPNs on the Internet. IPsec VPNs use the services defined within IPsec to ensure confidentiality, integrity, and authenticity of data communications across public networks, such as the Internet.

IPsec also has a practical application to secure WLANs by overlaying IPsec on top of cleartext 802.11 wireless traffic. When deploying IPsec in a

WLAN environment, an IPsec client is placed on every PC connected to the wireless network and the user is required to establish an IPsec tunnel to route any traffic to the wired network. Filters are put in place to prevent any wireless traffic from reaching any destination other than the VPN gateway and Dynamic Host Configuration Protocol (DHCP) or Domain Name System (DNS) server.

IPsec also provides for confidentiality of IP traffic, as well as authentication and anti-replay capabilities. Confidentiality is achieved through encryption using a variant of the Data Encryption Standard (DES), called Triple DES (3DES), or the new Advanced Encryption Standard (AES). Although IPsec is used primarily for data confidentiality and device authentication, extensions to the standard allow for user authentication and authorization to occur as part of the IPsec process.

3.2.1b Solution 2 : Implementing 802.1X / EAP

An alternative WLAN security approach focuses on developing a framework for providing centralized authentication and dynamic key distribution. This approach is based on the IEEE 802.11 Task Group “i” end-to-end framework using 802.1X and the Extensible Authentication Protocol (EAP) to provide this enhanced functionality. Cisco has incorporated 802.1X and EAP into its WLAN security solution—the Cisco Wireless Security Suite. The three main elements of an 802.1X and EAP approach follow:

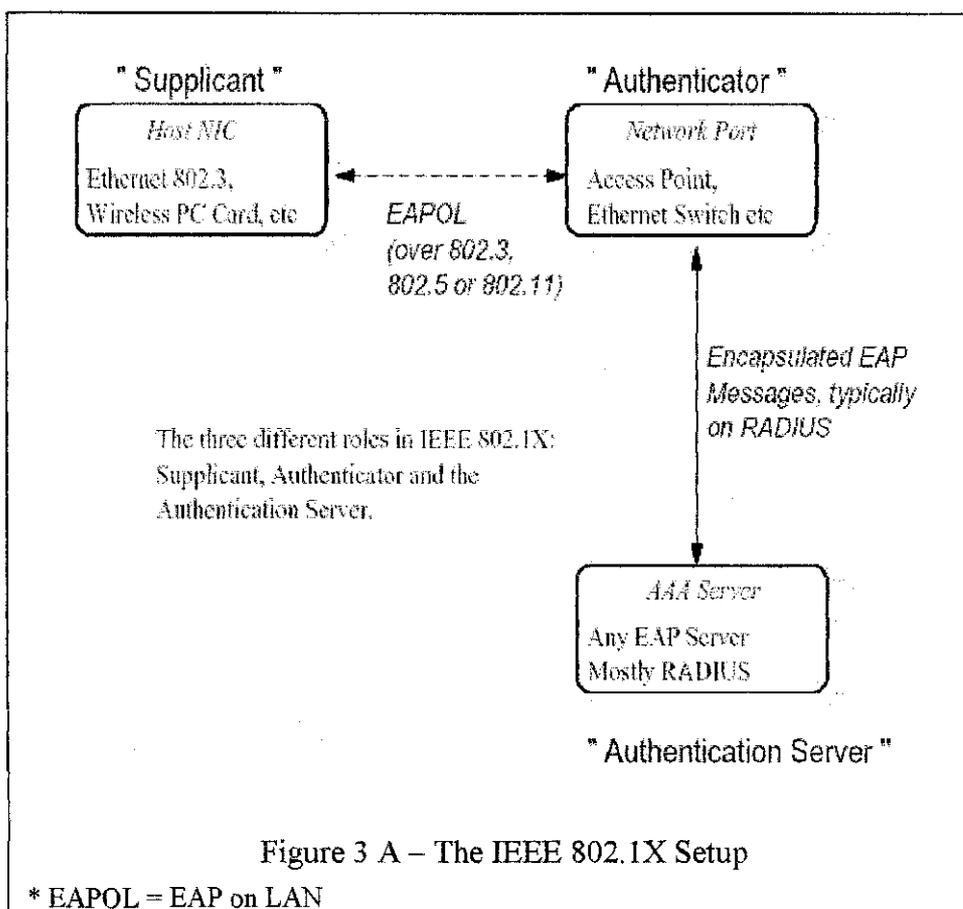
- Mutual authentication between client and authentication (Remote Access Dial-In User Service [RADIUS]) server
- Encryption keys dynamically derived after authentication
- Centralized policy control, where session time-out triggers reauthentication and new encryption key generation

When these features are implemented, a wireless client that associates with an access point cannot gain access to the network until the user performs a

network logon. After association, the client and the network (access point or RADIUS server) exchange EAP messages to perform mutual authentication, with the client verifying the RADIUS server credentials, and vice versa.

An EAP supplicant is used on the client machine to obtain the user credentials (user ID and password, user ID and one-time password [OTP], or digital certificate). Upon successful client and server mutual authentication, the RADIUS server and client then derive a client-specific WEP key to be used by the client for the current logon session. User passwords and session keys are never transmitted in the clear, over the wireless link.

After considering pros and cons for both solution, it is decided that 802.1x / EAP method is going to be used on the designed wireless network. Since IPsec is more toward utilizing Virtual Private Network.



Since we are choosing to use 802.1x / EAP as method to protect our network, we need to outline several basic guidelines to protect the network in terms of hardware setups :

- Access point security
 - Enable centralized user authentication (RADIUS) for the management interface.
 - Disable any insecure and nonessential management protocol provided by the manufacturer.
 - Limit management traffic to a dedicated wired subnet.
 - Isolate management traffic from user traffic and encrypt all management traffic where possible.
 - Enable wireless frame encryption where available.
 - Physically secure the access point. For example, putting it in a locked box or at unreachable places.

- Client security recommendations
 - Disable ad hoc mode.
 - In this mode, all wireless clients deployed a WLAN technology in a way that forms an independent peer-to-peer network, which is more commonly called an ad hoc WLAN. In an ad hoc WLAN, laptop or desktop computers that are equipped with compatible WLAN adapters and are within range of one another can share files directly, without the use of an access point.
 - When adapters use ad hoc mode, any hacker with an adapter configured for ad hoc mode and using the same settings as the other adapters may gain unauthorized access to clients

- Enable wireless frame encryption where available.

Devices required for this implementation

- *Wireless client adapter and software*—A software solution that provides the hardware and software necessary for wireless communications to the access point; it provides mutual authentication to the access point via an EAP mutual authentication type; an EAP supplicant is required on the client machine to support the appropriate EAP authentication type
- *Wireless access point*—Mutually authenticates wireless clients via EAP and can support multiple Layer 2 VLANs for user differentiation
- *Layer 2 or 3 switch*—Provides Ethernet connectivity and Layer 3 or 4 filtering between the WLAN access point and the corporate network
- *RADIUS server*—Delivers user-based authentication for wireless clients and access point authentication to the wireless clients; additionally, the RADIUS server can be used to specify VLAN access control parameters for users and user groups

DHCP server—Delivers IP configuration information for wireless LEAP clients

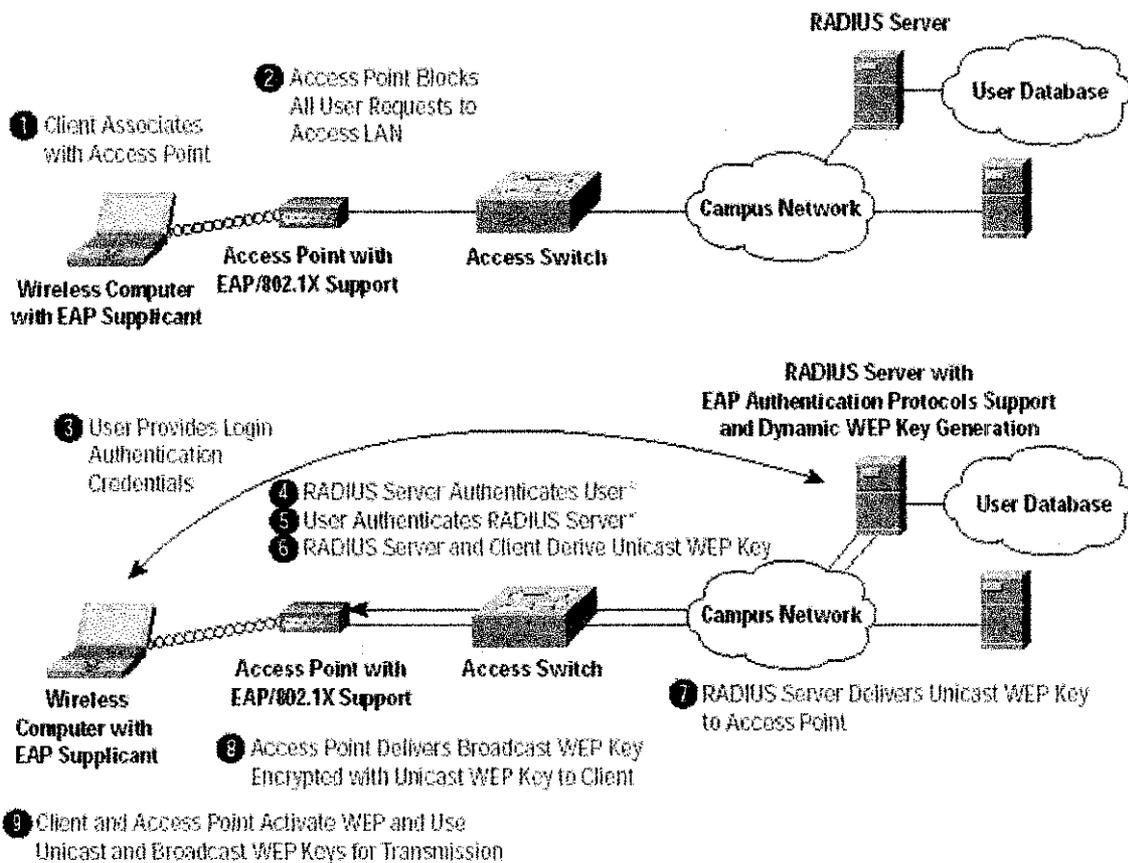


Figure 3 – B - Overview of suggested design of wireless LAN using 802.1X / EAP implementation.

In order to implement this technology, a RADIUS server is required to enable user account creation for user logins and verification of user before granted access into the Wireless LAN. Therefore a RADIUS server must be set up using a computer with Microsoft Windows 2000 Server installed.

This 802.1X / EAP implementation will be simulated in a network environment set within the Data Communication Lab.

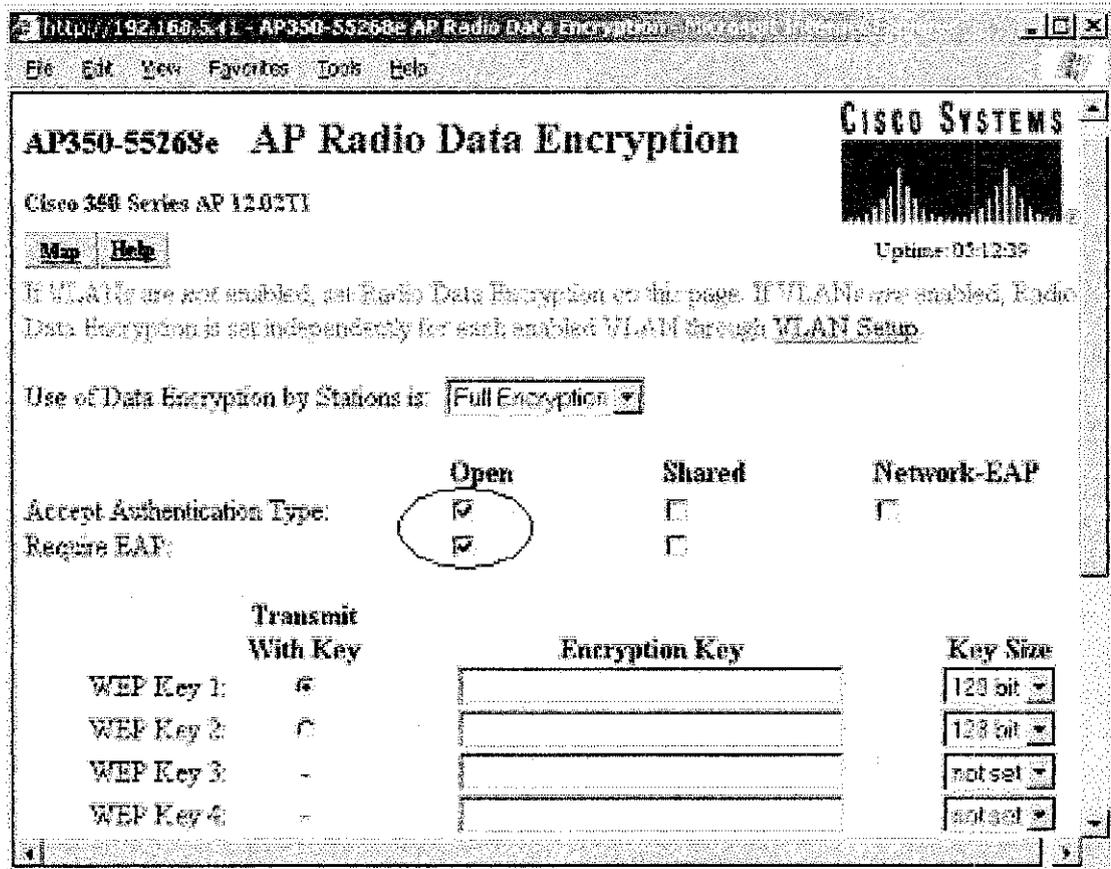


Figure 3 – C : Enabling Authentication on Cisco Aironet Access Points

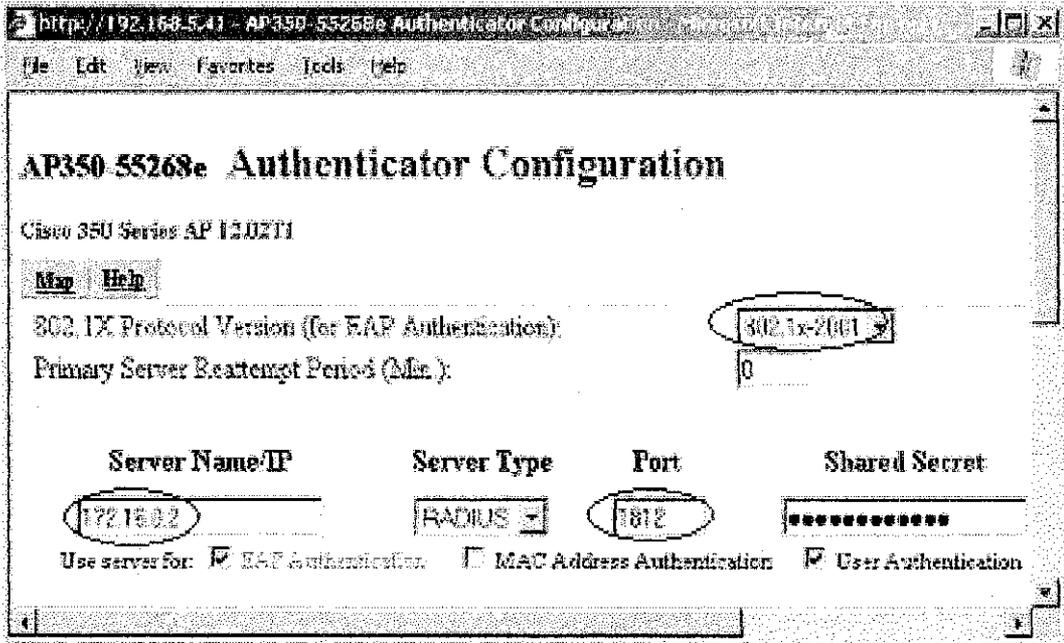


Figure 3 – D : Identifying the local RADIUS Server

CHAPTER 4

RESULTS AND DISCUSSION

Series of simulation and testing done in a network environment in Data Communication Lab to ensure the deployed Wireless LAN and RADIUS server performs as expected.

Equipment used :

- 3 (three) Unit of PC , installed with Microsoft Windows 2000 Server ;
 - DC 1 – acting as a domain controller, a Domain Name System (DNS) server, a Dynamic Host Configuration Protocol (DHCP) server, and a certification authority (CA).
 - IAS 1 - acting as a Remote Authentication Dial-in User Service (RADIUS) server.
 - IIS 1 - acting as a Web and file server.
 - Client1 – workstation functioning as wireless – connected client.
- 1 (one) unit of Wireless AP , a Cisco AP350 Wireless Bridge
- 1 (one) unit of Ethernet switch to provide connectivity to the outside network

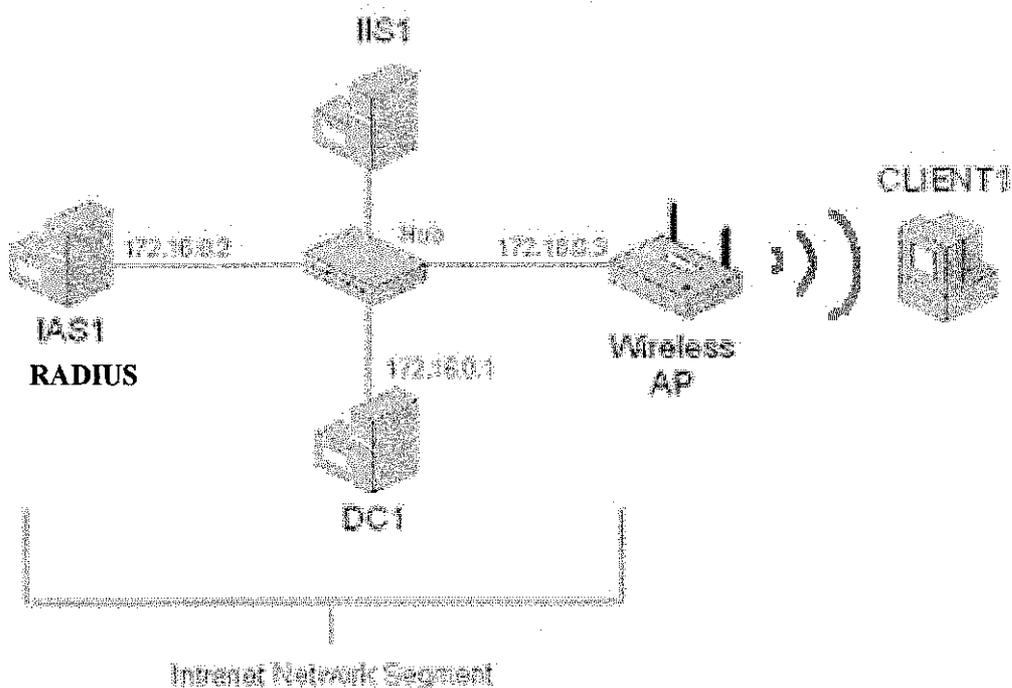


Figure 4 – A : Test environment for 802.1X / EAP Solution

After the network designed as above fully attached, configurations are done on the RADIUS server to enforce security aspect of the system, for example here, creating legit user account for users to log in into the Wireless LAN.

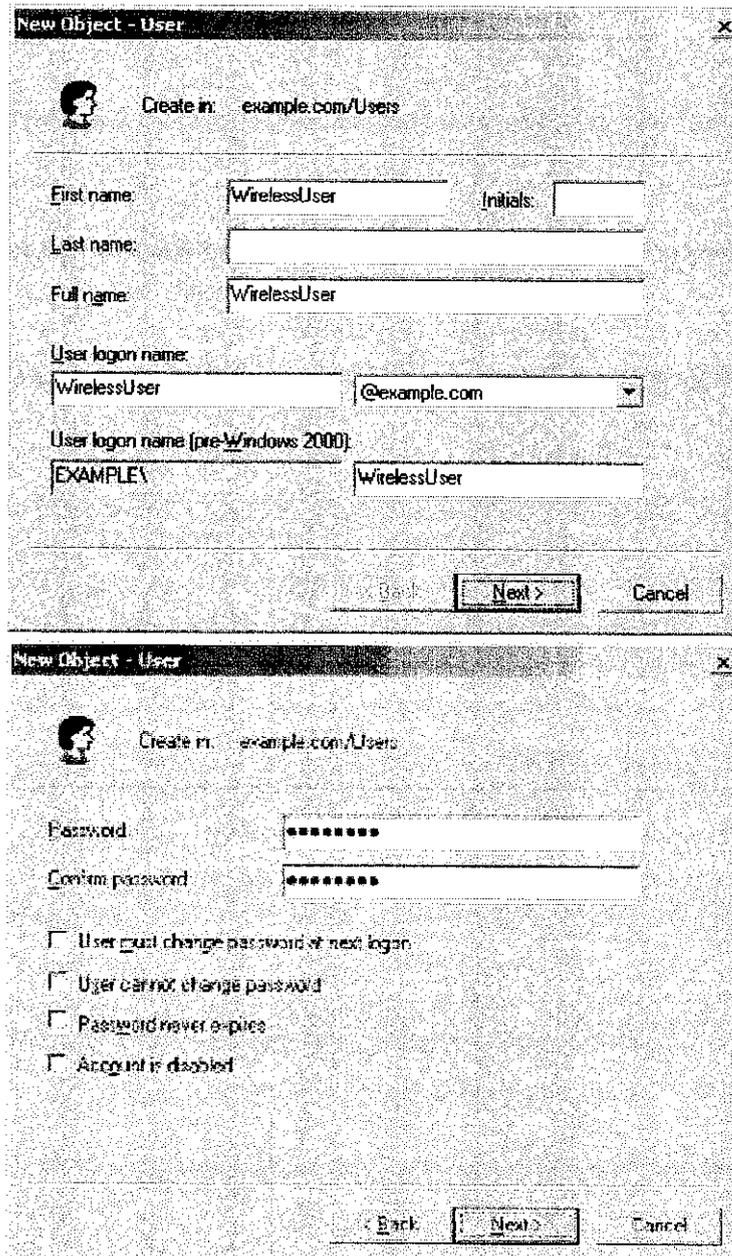


Figure 4 – B : Creating User Account on the RADIUS Server

In addition of creating user account, RADIUS server is also configured for access permission for each users that had been created earlier, for example here, user created under domain users is given read, enroll and auto enroll access only.

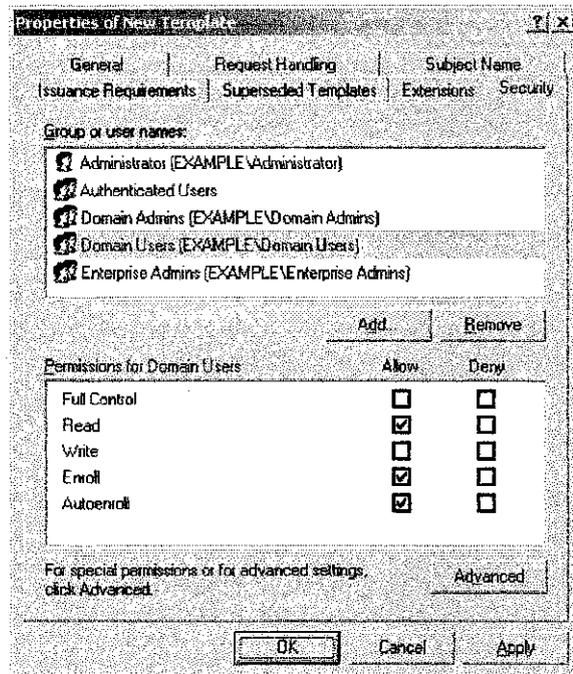
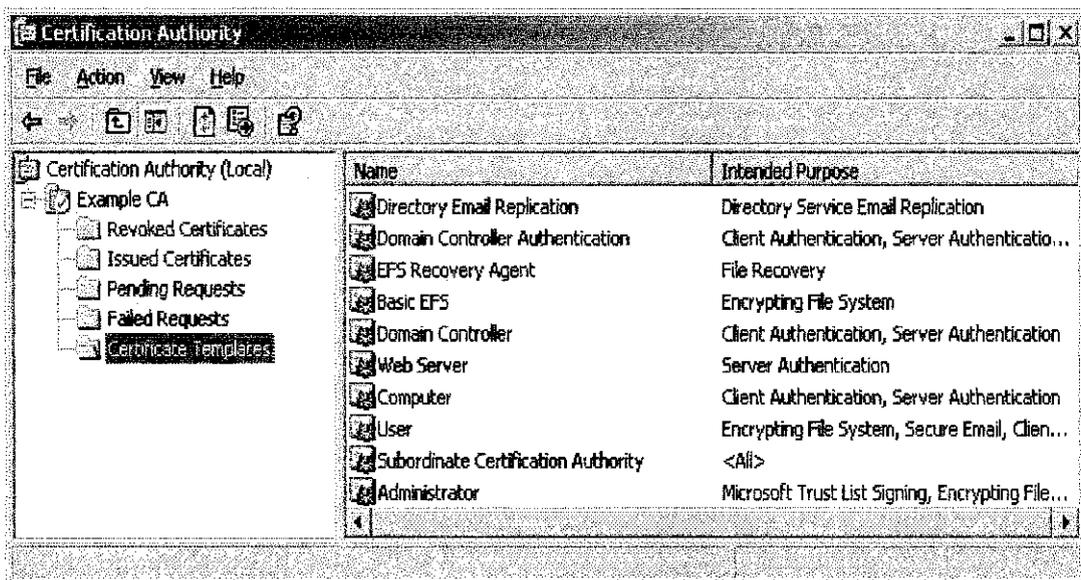


Figure 4 - C : Setting Up User Access Permission

Besides creating account, the RADIUS server also configured for certificates authentication to secure the network from unwanted users.



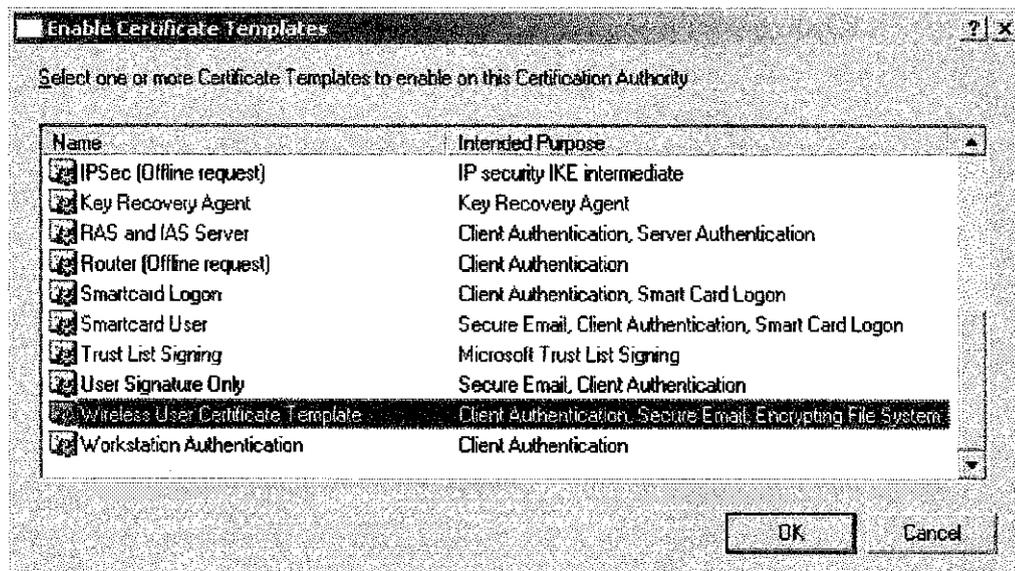


Figure 4 – D : Setting Up Certification Authority

Where as at the client side, upon successful connection to the WLAN, users need to reconfigure the security setting of their connection before the connection is re-connected using 802.1X / EAP protocol.

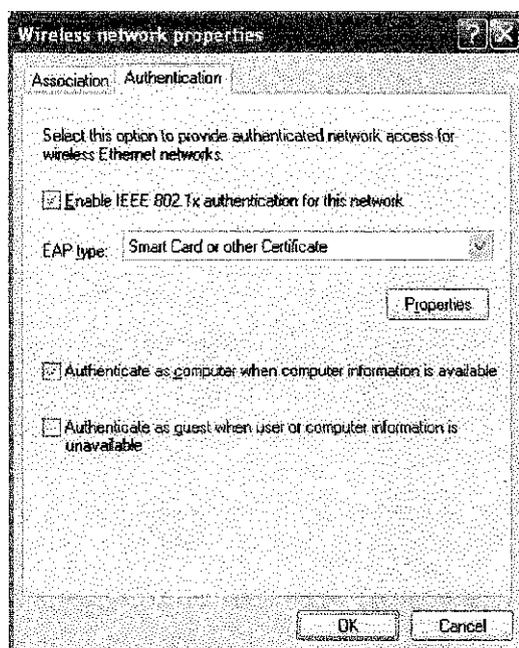


Figure 4 – E : Changing the Security Setting of the connection

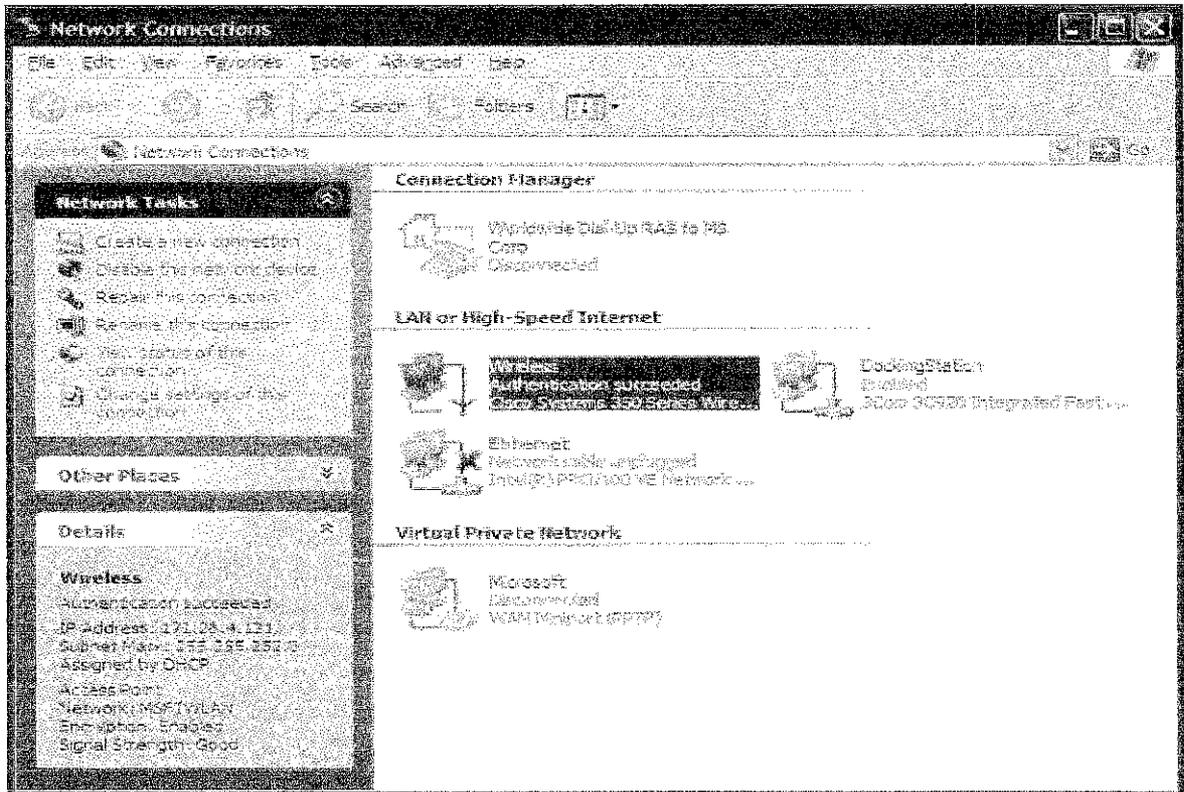


Figure 4 – F : Successful reconnected using 802.1X / EAP protocol using a Cisco 350 AP series

After using the mentioned 802.1X / EAP implementation and design and tested using series lab simulation, three significant benefits are realized through this implementation:

- The first benefit is the mutual authentication scheme, as described previously. This scheme effectively eliminates “man-in-the-middle (MITM) attacks” introduced by rogue access points and RADIUS servers.
- The second benefit is a centralized management and distribution of encryption keys. Even if the WEP implementation of RC4 had no flaws, there would still be the administrative difficulty of distributing static keys to all the access points and clients in the network. Each time a wireless device was lost, the network would need to be re - keyed to prevent the lost system from gaining unauthorized access.
- The third benefit is the ability to define centralized policy control, where session time-out triggers re - authentication and new key derivation.

From the implemented design also, the architecture able to mitigate some threats exposed to WLAN as followed:

- *Wireless packet sniffers* - Wireless packet sniffers can take advantage of any of the known WEP attacks to derive the encryption key. These threats are mitigated by WEP enhancements by key rotation using EAP.
- *Unauthenticated access*—Only authenticated users are able to access the wireless and wired network. Optional access control on the Layer 3 switch limits wired network access.
- *MITM*—The mutual authentication nature of several EAP authentication types combined with the Message Integrity Check can prevent hackers from inserting themselves in the path of wireless communications.
- *IP spoofing*—Hackers cannot perform IP spoofing without first authenticating to the WLAN, after authenticating on the Layer 3 switch restricts any spoofing to the local subnet range.

- *Address Resolution Protocol (ARP) spoofing*—Hackers cannot perform ARP spoofing without first authenticating to the WLAN; after authenticating, ARP spoofing attacks can be launched in the same manner as in a wired environment to intercept other users' data.
- *Network topology discovery*—Hackers cannot perform network discovery if they are unable to authenticate. The attacker can note that a WLAN network exists by looking for or observing the access point SSID, but cannot access the network. When authenticated via EAP, standard topology discovery can occur in the same way that is possible in the wired network.

However, the designed WLAN is still exposed to another threat which is

Password attack—Several EAP types take into consideration that an attacker can passively monitor the 802.1X/EAP exchanges between the client and the access point, and they (EAP) mitigate this risk via various methods.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

As wireless Local Area Network became one of the big thing during this recent years, everyone especially big firms are jumping into the WLAN bandwagons in order to increase their staff mobility within their organization and improve productivity. However, most of the organization jumped into the bandwagon without considering the utmost secret of their business, the network security. This will greatly jeopardize the safety of a company or organization and their secrets, at the same time putting the users that utilizing the network exposed to dangerous threats.

However, with proper planning and guidelines to be followed, a safe approach to implement wireless LAN is just a step away from hastily set up a WLAN. Extra efforts needed to ensure the safety of the organization that used this WLAN and also the connected clients by doing all the crucial steps as mentioned previously in this report.

5.2 Future Recommendation

The discussed implementation still has a few weaknesses which can be improved in the future, for example :

- We may still consider enabling static WEP keys on all devices in an effort to add an additional deterrent against hackers. The management overhead of dealing with static key changes makes this alternative less than ideal for large WLAN deployments. This management overhead could be mitigated by never changing the static WEP key, but this solution falls strongly into the “security-through-obscurity” category.
- Additionally, we can also consider using a layering of 802.1X/EAP with the IPsec-based VPN deployment to secure their WLAN environment. The primary drawback with this alternative is the necessity of managing two separate security infrastructures for WLAN deployments.
- To further secure the DNS and DHCP services, network designers should consider using dedicated hosts for the VPN WLAN DHCP and DNS deployment. This mitigates against two potential threats that could affect wired resources:
 - DoS attacks against the DHCP and DNS services that could affect wired users
 - Network reconnaissance through the use of DNS queries or reverse lookups

At the same time, in order to provide services to secure the WLANs, the status of the RADIUS server is crucial based on the following elements

- *Requests per second*—The Remote Access Dial-In User Service (RADIUS) server hardware and software must be able to accommodate the projected number of new RADIUS requests per second that will be offered by introducing WLANs. If the RADIUS servers are overburdened, wireless access point and VPN gateways will not be able to authenticate users, denying wireless users connectivity to the corporate network. Also, it should be noted that if the network designer elects to use a back-end database for user authentication, the back-end

database must also be designed to accommodate the projected number of user authentication requests per second that will be offered by introducing WLANs.

- *Redundant server deployment*—Multiple RADIUS servers should be deployed in order to give the authenticating device (wireless access point or VPN gateway) redundant options for servicing authentication requests. Network designers should also group the authenticating devices to alternate the listing of primary and secondary RADIUS servers. This setup accomplishes two goals: it limits the failure domain in the case of a server failure and also enables each RADIUS server to scale more effectively.

User management—RADIUS servers need to provide high-availability access to the user database required for user authentication. Network designers should consider implementing servers that synchronize data if the user database is to be stored locally. This setup allows a single point of administration and eliminates the possibility

REFERENCES

LITERATURE :

Nikita Borisov, David Wagner : Intercepting Mobile Communications: The Insecurity of 802.11

<http://www.isaac.cs.berkeley.edu/isaac/mobicom.html/>

Sean Convery, Darrin Miller , CISCO SAFE : Wireless Security in Depth whitepaper

http://www.cisco.com/en/US/netso1/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b3.shtml/

SAFE VPN: IPsec Virtual Private Networks in Depth:

http://www.cisco.com/warp/public/cc/so/cuso/eps0/sqfr/safev_wp.htm

Arunesh Mishra, Arbaugh William, Feb 2002, (Department of Computer Science, University of Maryland) : An Initial Security Analysis of the IEEE 802.1X standards

Using the Fluhrer, Mantin, and Shamir Attack to Break Wired Equivalent Privacy (WEP):

http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

Peter Rysavy, "Wireless Broadband and Other Fixed-Wireless Systems." CMP Media, Inc.

Tiho Vukasinovic, ITToolbox.com author

http://wireless.ittoolbox.com/browse/frameheader.asp?r=/pub/wireless_overview.htm&c=WirelessPeerPublishing&st=Wireless