

Hotspot in UTP

by

Nishalini Karunagaran

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

JUNE 2004

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

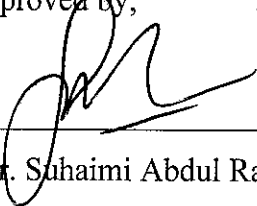
Hotspot in UTP

By

Nishalini Karunagaran

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

Approved by,



(Mr. Suhaimi Abdul Rahman)

UNIVERSITI TEKNOLOGI PETRONAS

Bandar Seri Iskandar

31750 Tronoh

Perak Darul Ridzuan

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 original work contained herein have not been undertaken or done by unspecified sources or persons.

Nishak

(NISHALINI KARUNAGARAN)

ABSTRACT

In today's world, it is necessary for organizations especially educational institution to keep up with the latest trend in technology. Technology changes practically everyday and it is important for these organizations to explore the world of technology. The latest hit on the market will be the Wi-Fi (wireless fidelity) fever. Hotspot is created using this Wi-Fi technology. Hotspot is a specific geographic location in which an access point provides public wireless broadband network service to mobile visitors through a WLAN. The main objective of this project is to do a research on hotspot and establish a wireless environment to support the theories provided in this documentation. This facility is provided for those with laptops and PDAs with wireless PC Card attached to them. Their machines will be free from any cables or wires connecting to the network port. They are basically mobile users and wireless LAN is ease to use as special terminal or OS is not required to access the network. In the methodology chapter, author discusses on the stages of development cycle used in conducting the study and research on the project. The results and findings discusses on authors conclusions and research diversion regarding the effort on establishing a hotspot in UTP. Author indicates the succession of the research in forming a wireless environment and the factors involved in setting up the Hotspot. The conclusion discusses on authors achievement in implementing hotspot and also the future upgrades suggested by author herself in order to improvise the research study in future.

ACKNOWLEDGEMENT

I would like to take this opportunity to thank those who have helped make this project a success. First and foremost, I would like to acknowledge God for it is through Him that I garner the strength to proceed during times of difficulty. I would also like to thank my parents for their unwavering support and encouragement. They have been and always will be there for me through thick and thin and for that I will be eternally grateful. I would also like to extend my greatest gratitude to my supervisor, Mr. Suhaimi Abdul Rahman, for his guidance and support throughout the duration of this project. Coupled with your patience and understanding, I have managed to accomplish this task with minimum difficulty. Finally, I take this opportunity to thank all those who have helped me in one way or another in completing this task. Although I am unable to list down all your names, your assistance is greatly appreciated. Thank you.

TABLE OF CONTENTS

Certification	ii
Abstract	iv
Acknowledgement	v
Table of Contents	vi
List of figures	viii
List of tables	ix
Abbreviations	x
CHAPTER 1: INTRODUCTION	1
1.1 Background of Study	1
1.2 Problem Statement	4
1.3 Objectives and Scope of Study	6
CHAPTER 2: LITERATURE REVIEW AND THEORY	8
2.1 Colleges sees the benefit of wireless access.....	8
2.2 Wireless Network Frees Student from Computer Labs.....	10
2.3 Wireless LAN (WLAN) Campus.....	12
2.4 Wireless vs. Wired Network in Education.....	15

CHAPTER 3:	Methodology or Project Work.....	17
	3.1 Methodology.....	17
	3.2 Project Identification.....	
	3.3 Tools Required	30
CHAPTER 4:	Results and Discussion	34
	4.1 Wireless LAN Specification.....	34
	4.2 Encryption (WEP).....	36
CHAPTER 5:	Recommendation and Conclusion.....	39
	5.1 Recommendation	
	RADIUS	39
	5.2 Conclusion	42
REFERENCES		44
APPENDICES		46
	1.0 Questionnaire	
	2.0 Network Diagnosis	

LIST OF FIGURES

- Figure 1 Basic Concept of Wireless Infrastructure Network**
- Figure 2 Sample of University Network**
- Figure 3 Bar Chart of Survey**
- Figure 5 Wireless LAN Security Level**
- Figure 6 Process Flow Diagram of System**
- Figure 7 Process Flow Diagram of User**
- Figure 8 Structure of Hotspot**
- Figure 9 Sample Express Setup Page (Bridge)**
- Figure 10 VLAN Setup Page**
- Figure 11 Data Encryption Page**
- Figure 12 Addressing Filters Page**
- Figure 13 Authentication Sketch**
- Figure 14 Radio Diagnosis Page**
- Figure 15 WEP Key Example**

LIST OF TABLES

Table 1 **IEEE Standards**

Table 2 **Methodology**

Table 3 **Results of Survey**

ABBREVIATIONS

AP	Access Point
ACL	Access Control List
DHCP	Dynamic Host Configuration Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Medium Access Layer
RADIUS	Remote Authentication Dial-In User Service
SSID	Service Set Identifier
UTP	University Technology Petronas
WDA	Wi-Fi Protected Access
WEP	Wired Equivalent Privacy
WAN	Wide Area Network
WLAN	Wireless Local Area Network

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Hotspot technology is currently spreading widely across the network world. As we can see, many appliances are going online, not only computers but also equipments such as hand phones and fax machines. Well, looking into this matter is it efficient enough to use wired network when we can switch to a hassle free mode – the wireless environment.

Many companies and institutions are acquiring network connections to access to the internet. But looking into the traditional process, they have to be connected via network cables. Cables have to be laid and port has to be assigned to each computer or other electrical appliances in order for user to get online. Well, laying out cables do acquire time and cost and in addition to that we will have user to access internet at a static mode.

Looking into this matter, academic institutions, especially one as commercial as University Technology Petronas, should allow its students and staffs to go mobile in accessing to the network. Many other institutions and companies (example :Starbucks and Kolej Damansara Utama) have acquired wireless technology and thus enjoy a mobile online connection that allows user to access network without having to look for ports and network cables. So why not a Hotspot for UTP?

1.1.1 What is Wireless LAN Networking

A Wireless Local Area Network (WLAN) is a flexible data communications system that can either replace or extend a wired LAN to provide added functionality. A traditional, wired local area network (LAN) sends packets of data from one piece of equipment to another across cables or wires. A wireless local area network (WLAN) relies instead upon radio waves to transfer data. Data is superimposed onto a radio wave through a process called modulation, and this carrier wave then acts as the transmission medium, taking the place of a wire.

The importance of WLAN technology, however, goes far beyond just the absence of wires. The advent of the WLAN opens up a whole new definition of what a network infrastructure can be. No longer does an infrastructure need to be solid and fixed, difficult to move, and expensive to change.

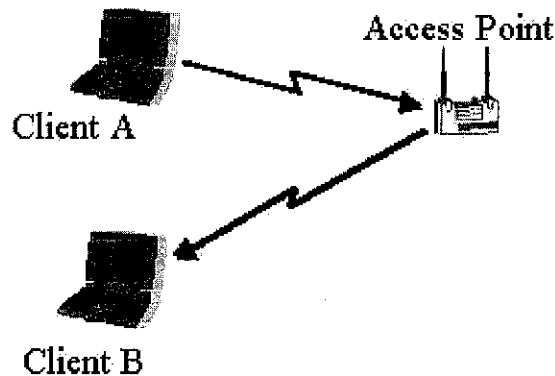


Figure 1 : Basic Concept of Wireless Infrastructure Network

1.1.2 What is hotspot?

Hotspot is a term for a location that offers Wi-Fi wireless internet access to the public. A Hotspot is created by setting up a wireless network that uses the 802.11 standards. Multiple users, with a wireless enabled device like a laptop or PDA, within range of the base station's broadcast signal can share a broadband connection to get online at the same time, and best of all, at very fast speeds.

1.1.3 What is wireless LANs Standards

The WLAN standards were started with the 802.11 standard, developed in 1997 by the IEEE (Institute of Electrical and Electronics Engineers). This base standard allowed data transmission of up to 2 Mbps. Over time, this standard has been enhanced. These extensions are recognized by the addition of a letter to the original 802.11 standard, including 802.11a and 802.11b. The chart below details the various standards related to 802.11.

802.11	The original WLAN Standard. Supports 1 Mbps to 2 Mbps.
802.11a	An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.725 GHz to 5.850 GHz) with a maximum 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz frequency, because the 802.11a specification offers more radio channels than the 802.11b. These additional channels can help avoid radio and microwave interference.
802.11b	-International standard for wireless networking that operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835 GHz) and provides a throughput of up to 11 Mbps. This is a very commonly used

	frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz frequency band. This is the current wireless technology approved by the government.
802.11e	Address quality of service requirements for all IEEE WLAN radio interfaces.
802.11f	Defines inter-access point communications to facilitate multiple vendor-distributed WLAN networks.
802.11g	Similar to 802.11b, but this standard provides a throughput of up to 54 Mbps. It also operates in the 2.4 GHz frequency band but uses a different radio technology in order to boost overall bandwidth.
802.11h	Defines the spectrum management of the 5 Ghz band for use in Europe and in Asia Pacific.
802.11i	Address the current security weaknesses for both authentication and encryption protocols. The standard encompasses 802.1X, TKIP, and AES protocols.

Table 1 : IEEE Standards

1.2 Problem Statement

1.2.1 Problem Identification

There are thousands of students studying in UTP and the amount of labs provided here is not sufficient enough to accommodate all the students at once. Labs are only open during office hours and students who are not staying at Villages are not able to get connected to the network. As a solution, alternatives should be given to students and according to my perspective; UTP should provide hotspot in UTP. With hotspot, those who have wireless card in their machine will be able to access the network without any

cables attaching to it. This facility will be very helpful when it comes to group project because the lab will be congested if all the students cramp the lab.

1.2.2 Significant of the Project

A hotspot is a limited-distance wireless LAN (WLAN) with the public access using IEEE 802.11 standard technology. As for this project, the standard which is being used will be the 802.11b. This international standard for wireless networking operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835 GHz) and provides a throughput of up to 11 Mbps. This is a very commonly used frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz frequency band. Furthermore, is the current wireless technology approved by the Malaysian government.

Access can be accomplished from notebook, PDA's and eventually mobile phones in the near future which have built-in wireless support feature or equipped with optional wireless devices. According to research done here at UTP, the students are supportive about the idea of implementing a hotspot here. Furthermore, students will experience the "always on" connection within the coverage area. The closer a student's machine to the wireless access point, the stronger of signal and connectivity it has. Besides, UTP should be in par with other institutes as WI-FI is the latest hit in current technology.

1.3 Objectives and Scope of Study

1.3.1 Objectives

The objectives that are to be achieved by the end of this project:

1. To study the implementation of hotspot in UTP
2. Ways to secure the hotspot
3. The efficiency of hotspot

1.3.2 Scope of Study

The basic scope of study for this project will be to research about the current hit on technology market; Wi-Fi and how to implement hotspot in UTP. As there were positive encouragement from the students of UTP, the efficiency and need of hotspot is going to be tested in the data communication lab. Based on the results obtained from this project, the management of UTP can take this research into consideration before hotspot is officially implemented in UTP.

1.3.3 Relevancy of the Project

One of our main sources of information is from the network, either the internet or the intranet. We as students of UTP at times find it hard to communicate with each other if in case of emergence. Besides, teamwork is encouraged here in UTP and it is difficult for us in a group to rush into the labs to get connected to the network. Hotspot will be a good solution as these students will be able to access the network according to their leisure time. By providing this facility, it does not only help the students in UTP but UTP will also be one of the few universities in Malaysia offering this service to its students. As there is no full equipment to establish this hotspot in areas like cafes and

our UTP library, the foundation will be established in UTP's Data Communication Lab. Results of the efficiency and stability of the hotspot can be obtained once the wireless environment is established.

Besides that, building a hotspot here in campus has got its own advantages. To list a few will be:

1. Ease of installation – no cables involved.
2. Flexibility – with wireless network, students as well as the staffs of UTP can work anywhere, anytime.
3. Easy to deploy - Wireless networks are easy to set up providing benefits in areas whereas wiring is difficult to deploy.
4. High Performance - Today's wireless networks offer high performance and bandwidth to keep all your essential applications and transactions running.
5. Cost Effective - Implementations do not require the expense or maintenance of wiring
6. Protected (WEP) - Short for Wired Equivalent Privacy, a security protocol for wireless local area network.

CHAPTER 2

LITERATURE REVIEW

2.1 College sees benefits of wireless access

Petaling Jaya-based KDU, a private college, has been providing WiFi access to the Web for its staff and students since 2001. In the beginning, the access was first limited to the management and staffs of KDU. This step is taken to enable their staffs to be more efficient in their work. According to the sales and marketing manager, WiFi network has greatly benefited their department. Besides, sales and marketing teams typically use a customer relationship management application to help customers and potential students visualize the courses and information database. Now, KDU is providing the WI-FI access to its students.

There has been many enquiries to the college at any time of the day and having WI-FI is an advantage here. Having this facility, the staffs of KDU can dispense with having to connect cables to LAN (local area network) ports and this enables them to move around without being inhibited.

As for now, KDU owns 8 access points and a laptop computer equipped with WiFi NIC (network interface card) gains access to the Internet. For the backhaul to the Internet service provider (ISP), KDU leased two 2Mbps leased lines from Telekom Malaysia Bhd; adding that the second 2Mbps line is redundancy backup line. The hotspot within the college extends to common areas like the cafeteria, library and computer centre, as well as the main auditorium.

Besides accessing the internet, the students of KDU are very active in KDU's e-Community Network or KCN in short. The main purpose of this KCN is to encourage the students to connect to a common "cyber meeting point" . In other words, this can be considered a virtual community meeting place where the students and lecturers get together. Among the activities organized by KCN will be

- student-lecturer discussions
- upload their assignments
- download timetables and schedules

The main difference of those with laptops and desktop PC will be that students who have laptops have the advantages of being able to access the KCN anywhere, anytime. Some of the benefits received by students and officials of KDU are such as:

- Communication – Student lecturer discussion online, cyber meeting point for students
- Ease of study – uploading and downloading features (example; notes, assignments, time tables, schedules)
- Management – customer services, staffs efficiency at work
- Always Online – network accessibility from anywhere and anytime

2.2 Wireless network frees college students from computer labs

By Roger Harris, Scripps_Mcclatchy Western Service

Foreign students of California Lutheran University (CLU) strongly agree that access to a free wireless Internet network on campus makes it possible to keep on top of their hectic schedule and stay in touch with their respective families.

Sitton a foreign student would like to cramp his MBA studies into one very short year to be back to his hometown explains benefits that he gained from the wireless access in his campus. Among the advantages of this service to the foreign students will be:

- check my e-mail on my laptop whenever I want
- check assignment online as soon as professors upload it

The wireless network allows him to better organize his time, collaborate online with other students who are in other locations and more easily access data networks from various "hot spots" around campus. In addition to the buildings, CLU's wireless network is designed to provide access in various common areas outside where students can sit against a tree or spread a blanket in the grass and do some work. Commuter students will be able to work online between classes or whenever they like without scheduling their lives around the hours of the computer labs.

Going wireless makes sense because an estimated 30 percent of CLU students have laptop computers. It won't be long before virtually all students will have their own laptop, PDA or other portable computer. Students now do not have to make an appointment with the lecturer for product presentation. They just upload it and lecturers can advice them at any time without problem. Students are also encouraged to access the Internet via the wireless network during classes for extra reference.

Funding for the wireless network was provided in part by a grant from the W.M. Keck Foundation. To access the network, students, faculty and staff must have a CLU e-mail account and password and a wireless networking card.

California State University, Channel Islands (CSUCI), also is building a wireless network on its campus in Camarillo. At present, CSUCI's wireless network is available in a warehouse and is being installed in the library. As buildings on the campus are renovated the plan is to provide wireless Internet access.

Both universities are building Wi-Fi networks, meaning they are compatible with the popular 802.11b wireless technology.

2.3 Wireless LAN (WLAN) Campus

A private Michigan university uses Interlink Networks Secure.XS™ wireless LAN security software to authenticate and control all users attempting to access two different networks: the offsite network through wired connections, and the inside campus network through wireless LAN connections. The university wanted a security solution that would centralize the management of all network users and record all session activity to allow departmental charge-backs.

The Secure.XS software is located at the university, and seamlessly interfaces to the local Internet service provider's Network Access Servers (NASs), authenticating all network users, and allowing the university to easily manage their user database and secure the connection.

2.3.1 The Project Overview

The university wanted its local Internet Service Provider (ISP) to be able to access the security software through a firewall in order to send its authentication requests, and thus required that the security software be compatible with and interfaces to the ISP's network access servers. The network ties to a LDAP user directory, which runs on a Linux server. The LDAP directory stores all of the users' information about access rights, session time allowances and departmental roles.

2.3.2 Requirements

The university needed an authentication solution with the following requirements:

Network Access Control.

- User authentication was needed for all people attempting to connect to the network via wireless LAN, dial-up, firewall, and tunnel/VPN access. The university wanted a standards-based solution that would work with existing equipment and databases – not a proprietary, expensive solution.

Compatibility with the ISP's Hardware.

- Since all of the hardware equipment for the dial-in network was located offsite at the university's local ISP, solution compatibility and integration between that network and the university's on-site equipment was a major requirement. The ISP would have to access the security software through the university's firewall, to be granted authentication and access the user directory.

Easy to Use and Maintain.

- The IT department wanted to manage all network users via a simple, web-based interface – not through a complex command line-interface that the rotating network administrators would not know how to use.

Tight Security.

- With students and faculty access the network via multiple wired and wireless methods, and the ISP needing to proxy authentication requests to the authentication software to check user's credentials, security and privacy was a major concern.

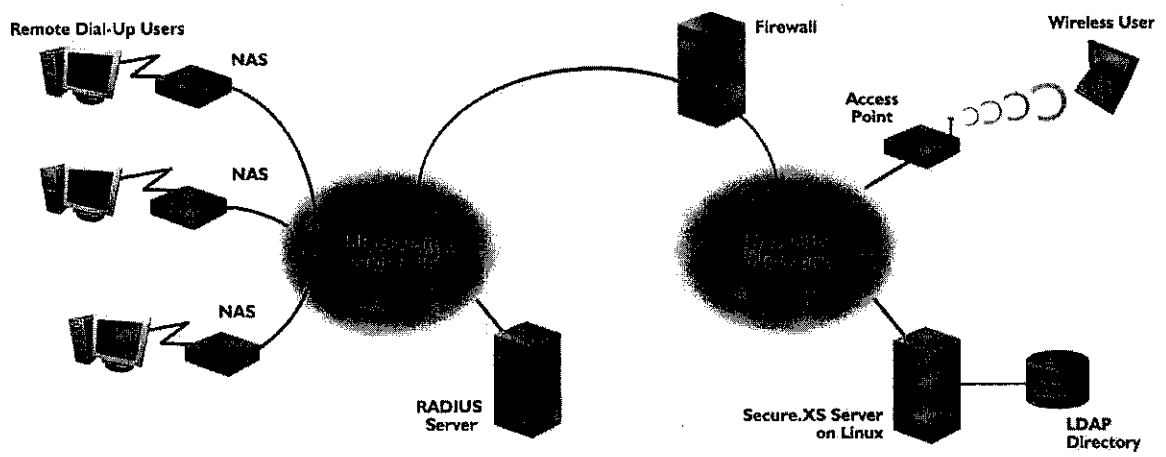


Figure 2 : Sample of University Network

2.4 Wireless vs. Hard-Wired Network Use in Education

By Dr. Sylvia Charp

Wireless local area networks (WLANs) are increasingly being used in education, with nearly two-thirds of institutions currently using WLANs in school districts. A WLAN is defined as a local area network, not connected by cables or wires, which uses a wireless technology to carry information between the nodes of the network. WLANs depend on the number and configuration of access points for their functionality. Wireless access points are positioned so students can move desks around during classroom projects and so teachers can move from room to room. Also, learners can connect their computers anywhere on campus where there is proximity to an access point.

Benefits of wireless include

- **Flexibility.** In older buildings, re-wiring is not always an option due to the physical restraint of the building. Also, existing space may not allow traditional cabling.
- **Ease of use.** Installing a WLAN requires less physical work than installing or adding to a LAN. WLANs have also increased communication and encouraged spontaneity.
- **Mobility.** WLANs allow users to move freely around the room, to wherever access points are in operation.
- **Cost.** For general use, a WLAN does not save much money. The cost of network interface cards increases from about \$67 for a standard card to about \$180 for a wireless type. However, the overall investment in WLAN is less expensive than retrofitting cables into old buildings.

2.4.1 Standards and Security

WLANs have been functioning in recent years using several standards. Recently two variations of standards are in use for implementing WLANs. IEEE 802.11b, known as Wi-Fi, is the more mature standard, though it has a relatively slow transmission speed. The major weakness of the Wi-Fi standard lies in its security, with only very basic protection of the data being transmitted.

Arguments for WLANs are most convincing when renovation is needed and the cost of construction is high. However, the cabled network operates at speeds much faster than the wireless network. Faster processing, more memory, better displays and some degree of standardization are all listed as advantages of LANs. So, it seems both wireless and hard-wired technologies have their place in the educational environment.

CHAPTER 3

METHODOLOGY/PROJECT WORK

3.1 Methodology

In order to develop any projects, proper methodology has to be outlined. There are 6 basic phases in doing this project. All the phases are summarized in the table below:

NO.	PHASE	ACTIVITIES
1.	Observation	<p>Observation</p> <ul style="list-style-type: none">○ Observe the percentage of usage of the network○ Observe the frequency of network usage <p>Selection</p> <ul style="list-style-type: none">○ Find appropriate title○ Find appropriate location

Analysis

2.	Preliminary Information Gathering	<p>Mission of project</p> <ul style="list-style-type: none"> ○ Define problem statement, objectives and scope of study <p>Information Gathering</p> <ul style="list-style-type: none"> ○ Data collected from various resources <ul style="list-style-type: none"> - internet - books and magazines ○ Depth study and Analysis <ul style="list-style-type: none"> - literature review 	} Analysis
3.	Data Analysis	<p>Compilation of information</p> <ul style="list-style-type: none"> ○ analyze all relevant data ○ come up with an idea of how to build a hotspot 	
4.	Design	<p>Sketch the design</p> <ul style="list-style-type: none"> ○ Basic diagram of how the network should look like ○ Sketch the process flow diagram 	} Design
5.	Development	<p>Build hotspot</p> <ul style="list-style-type: none"> ○ Build the hotspot in UTP according to the network design 	
6.	Testing	<p>Test hotspot</p> <ul style="list-style-type: none"> ○ Test the efficiency and reliability of the service 	} Testing

Table 1 : Methodology

3.1.1 Analysis

3.1.1.1 Phase 1 – Observation

According to my observation, students find it hard to get connected to the network after office hours. This is because all the labs are closed after 5 pm. Most of the students can only have their group project discussion after classes and by the time their classes are over, labs are already closed. Network is essential to all students regardless whether it is for purely research or it is for communication purposes. A 24 hours connection should be provided for the students to access their network. As a solution, since labs cannot be opened 24 hours a day, hotspot should be built in UTP to overcome this problem. To be more precise about my view, a small survey was conducted among the students on the future recommendation for hotspot. List of questions asked is attached at the appendix section. (1.0 Questionnaire).

3.1.1.2 Phase 2 – Preliminary Information Gathering

All the distributed questionnaires were collected to obtain the results of the survey. The table below shows the summarized results of the survey done.

QUESTION NO.	YES	NO
	(PERCENTAGE OF STUDENTS)	(PERCENTAGE OF STUDENTS)
1	20	30
2	50	0
3	5	45
4	50	0
5	50	0
6	50	0
7	43	7
8	37	13
9	41	9

Table 2 : Results of Survey

To put things into a clearer view, a bar chart is generated from the data gathered. By viewing data from the bar chart, the majority of students wanting hotspot service in UTP is very high. Below is the bar chart indicating the results of the survey

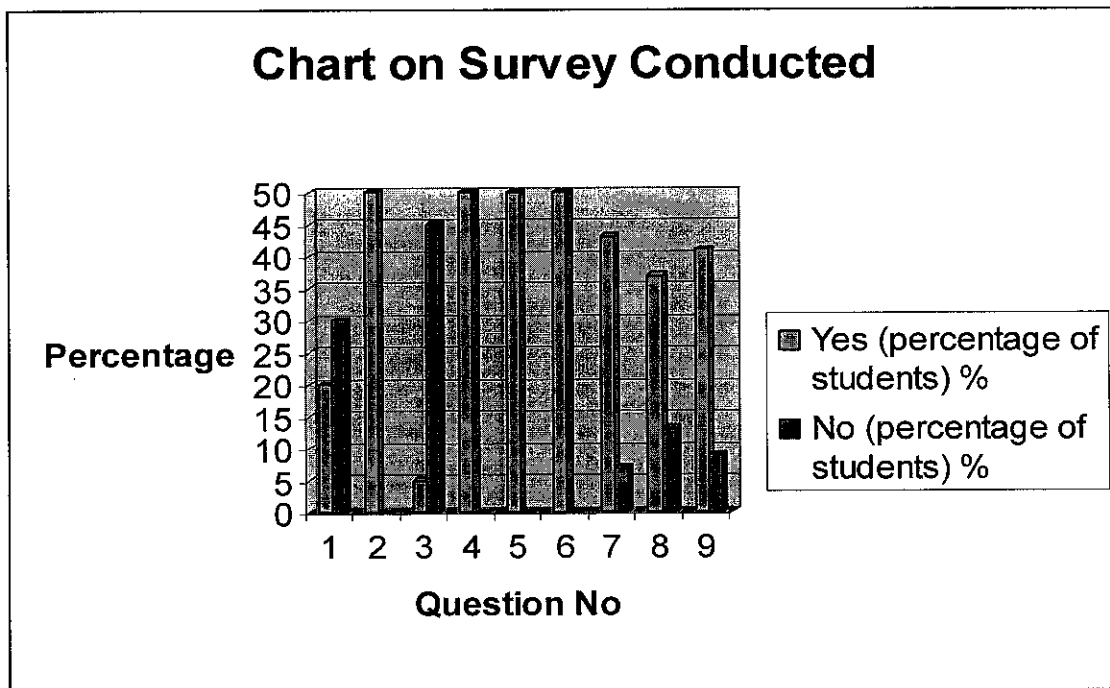


Figure 3 : Chart about Survey

After gathering sufficient data, mission and problem statement was identified so that the project will not run out of its scope of study. Once the objectives have been outlined, research was done according to the scope of study.

3.1.1.3 Phase 3 – Data Analysis

Once all information about the survey and research done was collected, analyzed the obtained information to see the relevancy of it to the project. The most crucial part of deploying a wireless environment will be its security. Ensuring adequate security should be our main concern. To list a few will be the following

1. ESSIDs

The very first security mechanism will be the Extended Service Set ID (ESSID), which is a alphanumeric code that is entered into the all APs and wireless clients that participate on the same wireless network. Changing the ESSID from its default value is a good first step towards heightened security. By disabling this broadcast, users either have to know the network name or have some kind of wireless packet captured software to derive the information.

2. WEP (Wired Equivalent Privacy)

Once a computer is granted access to the network, it's important to encrypt the data since data transmitted in the clear can be sniffed out. 802.11b provides an encryption mechanism known as WEP. WEP uses either a 64-bit or a 128-bit encryption key and is generally disabled by default on APs.

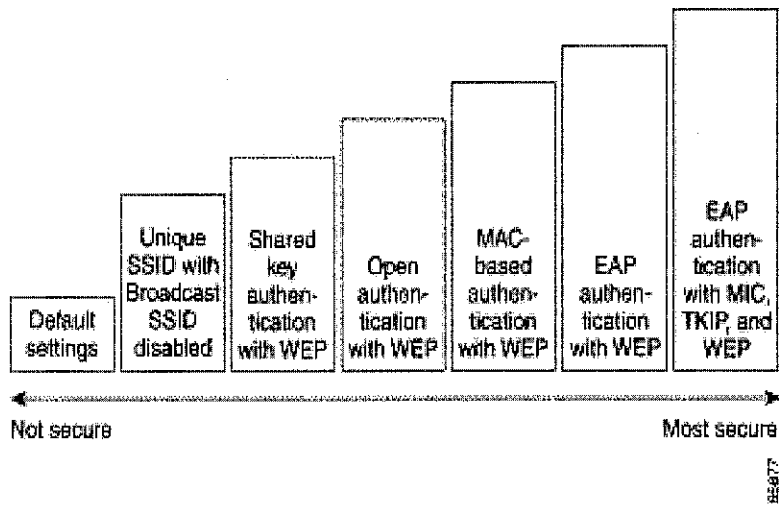


Figure 5 : Wireless LAN Security Levels

3.1.2 Design Phase

3.1.2.1 System and User Design

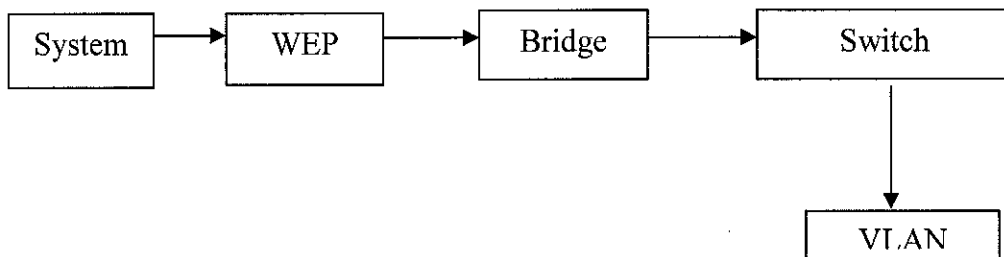


Figure 6 : Process Flow Diagram of the System

Once the user keys in the username and password as well as the WEP key, it will be sent to the authentication server to check whether that particular user has an account with UTP. Their account is basically their MAC address which has been stored in the MAC address filter. If their MAC address is not listed in the authentication server, then that particular user is not allowed to access the wireless network. If that particular user has been authorized, they will be given the liberty to access the VLAN of UTP.

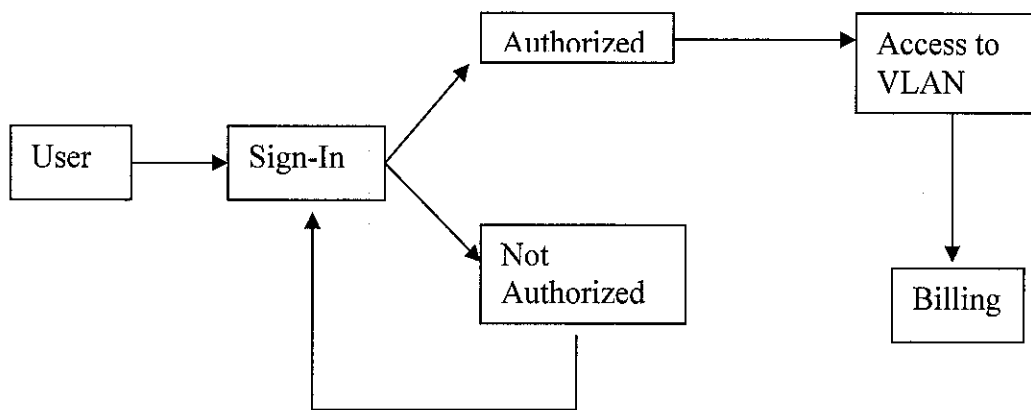


Figure 7 : Process Flow Diagram of the User

The user of this facility (student of UTP as well as the employees) will have to sign in order to access the wireless environment. They have to key in their MAC address as well as the WEP key. If their input is correct, they will be authorized to use the facility and if their input is wrong, they will not be able to get connected to the wireless environment. They have to re-login with the correct MAC address and their WEP key.

3.1.2.2 Hotspot Design

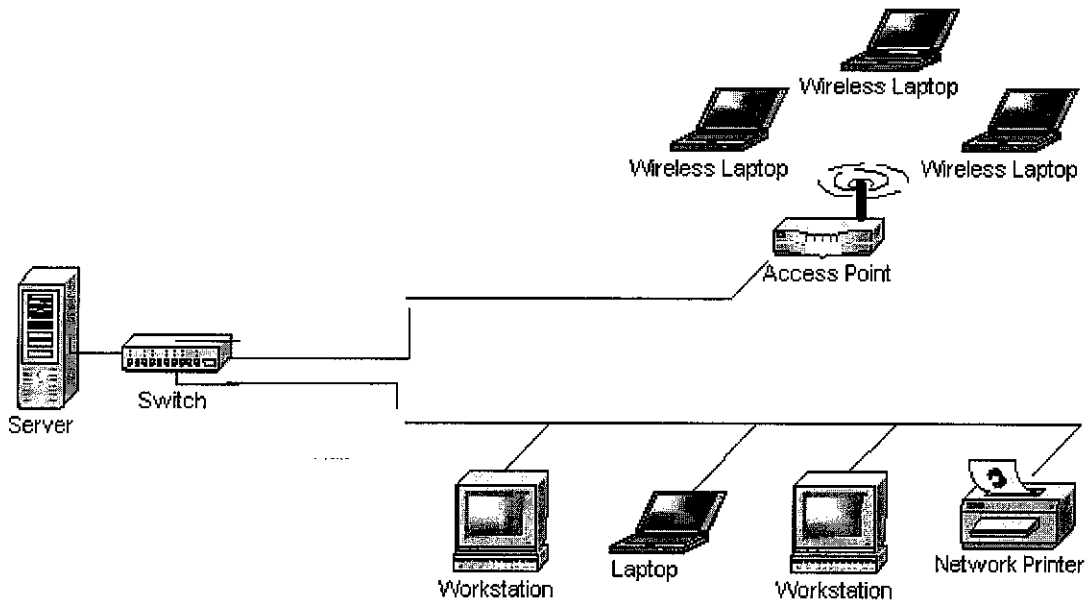


Figure 8 : The structure of the hotspot

The figure above shows the setting of a hotspot. Among the equipments that you need to have in building a hotspot will be the bridge, switch (bridge communicates with this switch to reach the server), and computer or laptop equipped with the wireless network card. Details about the equipments and tools used to build the hotspot will be discussed later. The access point is basically the heart of creating a hotspot. As, for this project, a bridge is used and the bridge is assigned to act as an access point. The bridge has to be configured to follow the 802.11 standards and this bridge will be divided into separate VLAN. This VLAN will be assigned to individual ports at the switch and the request will be sent to the server. IN order to access the server, user authentication and password is required. Once the authorization is successful, the user is free to navigate around the network.

3.1.2.3 Radio Configuration

System Name:	AP350-41c50a
MAC Address:	00:40:96:41:c5:0a
System Serial Number:	
<u>Configuration Server Protocol:</u>	None
Default IP Address:	192.168.141.41
Default IP Subnet Mask:	255.255.255.0
Default <u>Gateway:</u>	192.168.141.1
AP Radio:	
Service Set ID (SSID):	Guest more...
Role in Radio Network:	Root Access Point
Optimize Radio Network For:	<input checked="" type="radio"/> Throughput <input type="radio"/> Range <input type="radio"/> Custom
Ensure Compatibility With:	<input type="checkbox"/> 2Mb/sec Clients <input type="checkbox"/> non-Aironet 802.11
<u>Security Setup</u>	
<u>SNMP Admin. Community:</u>	admin1
<input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Restore Defaults"/>	

Figure 9 : Sample Express Setup Page (Bridge)

Output :

1. System Name
2. Configuration Server Protocol (DHCP)
3. Default IP and IP Subnet Mask
4. Default Gateway
5. Radio Service Set ID (SSID)
6. Radio Status

3.1.2.4 VLAN Configuration

VLAN Summary Status

VLAN (802.1Q) Tagging: Enabled Disabled
802.1Q Encapsulation Mode: Hybrid Trunk
Maximum Number of enabled VLAN IDs: 16
Native VLAN ID:
Single VLAN ID which allows **Unencrypted** packets: (0=all require encryptic
Optionally allow **Encrypted** packets on the unencrypted VLAN: yes no

VLAN ID: VLAN Name:

Existing VLANs:

1	Native VLAN
2	Full-Time
3	Part-Time
4	Guest
5	Maintenance
When VLAN Disabled	

Figure 10 : VLAN Setup Page

Output :

1. VLAN Name
2. VLAN ID
3. Establish WEP key for each VLAN type
4. Create SSID
5. Choose Authentication Type

3.1.2.5 Security Setting

If VLANs are *not* enabled, set Radio Data Encryption on this page. If VLANs *are* enabled, Radio Data Encryption is set independently for each enabled VLAN through VLAN Setup.

Use of Data Encryption by Stations is: Not Available
Must set an Encryption Key or enable Broadcast Key Rotation first

	Open	Shared	Network-EAP
Accept Authentication Type:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Require EAP:	<input type="checkbox"/>	<input type="checkbox"/>	

	Transmit With Key	Encryption Key	Key Size
WEP Key 1:	-		not set ▼
WEP Key 2:	-		not set ▼
WEP Key 3:	-		not set ▼
WEP Key 4:	-		not set ▼

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

Figure 11 : Root Radio Data Encryption Page

New MAC Address Filter:

Dest MAC Address:

Allowed Disallowed

The default settings for multicast and unicast destination MAC addresses transmitted from each network interface are specified on the Advanced Setup page for that network interface.

Existing MAC Address Filters:

Lookup MAC Address on Authentication Server if not in Existing Filter List?

yes no

Is MAC Authentication alone sufficient for a client to be fully authenticated?

yes no

40000

Figure 12 : Address Filters Page

Output :

Enter WEP username

Enter password

Figure 13 : Sketch of prompt interface for input

Once the user enter the WEP username and password, the information will be past to the authentication server. If both the WEP key is correct, that user is allowed to visit the wireless environment. Those who fail to provide the WEP key will not be able to access the wireless facility.

3.1.3 Testing Phase

Testing will be done using one of the notebook which is equipped with wireless network card. The network card must detect the signal from the access point in order for the user to be able to get connected to the wireless environment. The results obtained will indicate the status of the project.

One example of testing will be the network diagnosis test. The figure below show the main page that provide the radio diagnosis tests and provide links to the VLAN Summary Status and SSID statistic pages from access point radios.

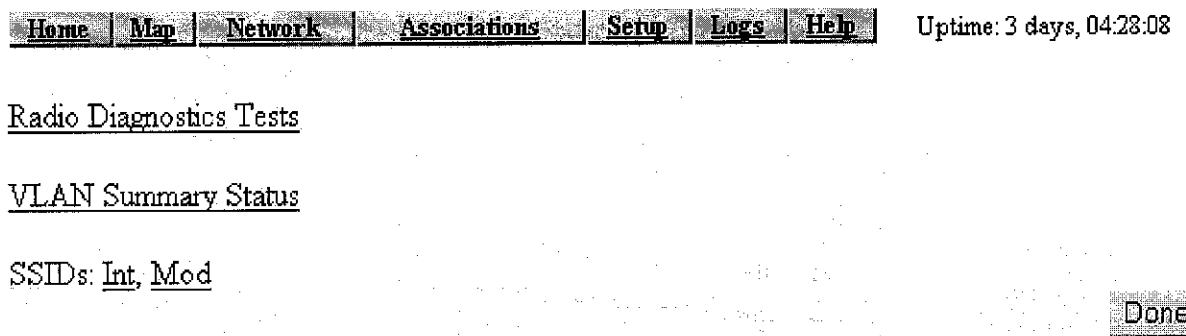


Figure 14 : Radio Diagnosis Page

3.2 Procedure Identification

In this basic procedure identification, all the phases described earlier are included in the following 3 steps in establishing a hotspot.

Step 1: Location

The *first step* in setting a location up for Wi-Fi is to install a high-speed broadband service. There are a number of ways you can subscribe for high-speed internet access, but the most popular 2 methods are through your existing cable or telephone lines.

Step 2 (a) : Wireless Equipment

The *second step* - PART A is to purchase wireless equipment. There are 2 items that will be needed to set up and use a wireless network. First, to set up the 'wireless cloud' you will need a Wireless Access Point. A wireless access point is simply a device that connects to your existing high-speed internet modem, and creates a wireless extension for an area of about 250 - 300 square feet. This is known as the 'wireless cloud' and represents the area of coverage that one must be in to access the Wi-Fi signal. The newest access points utilize 802.11G wireless technology, which is the standard wireless protocol recently ratified by the IEEE.

Step 2 (b): Wireless Equipment

The *second step* - PART B is to purchase a wireless adaptor. In PART A, the equipment purchased is necessary to DEPLOY the wireless signal. Now, buy the device that is necessary to RECEIVE this wireless signal. This is the piece of equipment that will be installed into your laptop or PDA, to enable it for wireless internet sharing.

Step 3 : Network Configuration

The *final step* is to configure the wireless access point and the wireless network adapter. These are the 2 products purchased in Step 2. The basic set up will go like this: CABLE OR TELEPHONE LINE --> CABLE OR DSL MODEM --> WIRELESS ACCESS POINT --> COMPUTER. Usually, one will install and configure the wireless access point first, by manually entering the relevant wireless network configurations (SSID Network ID, Channel, WEP Security Key, etc.). Once the access point is configured, one MUST match these settings onto the configuration utility of the network adapter. This is the device that installs into the laptop or PDA. When this is configured to match the access point settings, the hotspot is built.

3.3 Tools

Types of Equipment

- PC Card Radio
- Switch
- Bridge
- Hardware

1. PC Card Radio

Wi-Fi networks use a radio band to "broadcast" data to other Wi-Fi enabled equipment and the most common client device is the PC Card Wi-Fi radio. There are hundreds of variations, but most look like a standard Type II PC Card that slides into your laptop's PC Card slot. These cards used to be known as PCMCIA (Personal Computer Memory Card International Association) cards but are now simply called PC Cards.). AS for this project, I'm using the PC CARd produced by Cisco Systems.

The protruding end of most Wi-Fi PCCards contains a built-in antenna, usually a miniature twin that can sometimes spring out to improve coverage. Some of them have a tiny connector on the end to which you can attach a larger, more powerful antenna to maximize

On many laptop computers, the software and drivers for these PC Cards are already built in. If you are using Windows XP, you may find that when you slide in the card, the drivers and software will load automatically. The computer will then scan the area to find and log onto the closest Wi-Fi network.

2. Switch (Cisco Catalyst 3550 Series)

The Cisco Catalyst 3550 Series Switch is a stackable, multilayer switch that provides availability, quality of service (QoS), and security to enhance network operations. With a range of Fast Ethernet and Gigabit Ethernet configurations, the Cisco Catalyst 3550 Series is a powerful option for enterprise and metro access applications.

3. Bridge (Cisco Aironet 350)

The Cisco Aironet® 350 Series Wireless Bridge enables high-speed long-range outdoor links between buildings and is ideal for installations subject to plenum rating and harsh environments. It is designed to meet the requirements of even the most challenging applications, with features including:

- High-speed (11-Mbps), high-power (100-mW) radios, delivering building-to-building links of up to 25 miles (40.2 km)
- A metal case for durability and plenum rating and an extended operating temperature rating for harsh environments

- Supports both point-to-point and point-to-multipoint configurations
- Broad range of supported antennas
- Simplified installation, improved performance, and upgradeable firmware, ensuring investment protection

The bridge uses the DHCP protocol. The *Dynamic Host Configuration Protocol* (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information such as the addresses for printer, time and news servers.

4. *Hardware*

WLAN consist of two main building blocks including an access point that connects to the network and a wireless adapter installed in the computing device.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Wireless LAN Specification

A wireless local area network (Wireless LAN) is a computer network that allows a user to connect without the need for a network cable. A laptop or PDA equipped with a wireless LAN card lets a user move around a building with their computer and stay connected to their network without needing to “plug in” with a cable. The most popular wireless LAN today is called an 802.11b network.

Over here, there are 4 areas of concern which will be:

1. Coverage

Wireless local area networks by definition operate over a small, “local” coverage area, normally about 100 m in range. They are typically used in buildings to replace an existing wired Ethernet, or in a home to allow multiple users access to the same Internet connection. Other wireless LAN coverage areas can include public hotspot at cafes and libraries.

2. Speed

The 802.11b wireless LAN standard transfers data at speeds of up to 11 Mbps, with typical rates of between 1–4 Mbps, decreasing as more users share the same wireless LAN connection. The next version, 802.11a, is supposed to transfer

data at speeds of up to 54 Mbps. However, a potential problem for throughput is overcrowding of the bandwidth. Many people or businesses using wireless LANs in the same area can overcrowd the frequency band on which they are transmitting. Problems with signal interference are already occurring and airwaves may become overcrowded.

3. Data Security

802.11b networks have several layers of security, however there are weaknesses in all of these security features.

Security can be increased on wireless LANs by using shared key authentication. This shared key must be delivered through a secure method other than the 802.11 connection. In practice, this key is manually configured on the access point and client, which is not efficient on a large network with many users. This shared key authentication is not considered secure and is not recommended to ensure security.

Another weakness in an 802.11 network is the difficulty in restricting physical access to the network, because anyone within range of a wireless access point can send, receive, or intercept frames. WEP (Wired Equivalency Protocol) was designed to provide security equivalent to a wired network by encrypting the data sent between a wireless client and an access point.

However, key management is a significant problem with WEP. WEP keys must be distributed via a secure channel other than 802.11. The key is normally a text string that needs to be manually configured on the wireless access point and wireless clients, which is not practical to a large network. There is also no mechanism to change the WEP key regularly, so all wireless access points and clients use the same manually configured WEP. With several wireless clients

sending large amounts of data, without changing the WEP key, it is possible to intercept data traffic and determine the WEP key. This would allow a hacker to intercept and decrypt the data traffic.

Another problem that has been reported with wireless LANs is that when the security features are turned on, there are problems with interoperability between wireless LAN modules from one vendor and wireless LAN access points from another vendor.

Thus the objectives stated by the author;

- Ways to secure the hotspot (WEP)
- Efficiency of Hotspot (Coverage, speed), was able to be achieved.

4.2 Encryption (WEP)

WEP is an optional encryption standard. According to the protocol, WEP generally uses a 64-bit RC4 stream cipher. RC4 is a symmetric encryption algorithm, meaning the same key is used to both encrypt and decrypt the data payload. This encryption key is generated from a seed value created by combining a 40-bit user defined WEP key with a 24-bit Initialization Vector (IV). The WEP key generally takes the form of a 10-character hexadecimal string (0-9,A-F) or a 5-character ASCII string, which must be present on both ends of the wireless transmission. The protocol allows for up to four concurrently defined WEP keys.

The standard does not, however, currently define how the IV is established, so the implementation varies by vendor. When an encrypted wireless client starts transmitting data, the IV can start with a value of zero or another randomly defined starting value, and generally increments upwards in a predictable manner, with each successive frame. However, some vendors (such as Cisco) use a more sophisticated, random determination of the IV.

WEP encryption is performed at Layer 2 above the MAC sublayer, which means that only the data payload and header information from higher in the protocol stack are encrypted. The cipher text is formed from the IV+WEP key combination, the plaintext and the checksum. A series of WEP-related headers are then appended to the frame, including the IV value and which WEP key was used. Then other MAC sublayer information including destination and source addresses, in addition to the BSSID, are appended as well. All MAC related information in the header is transmitted unencrypted. The frame is then sent out, at which point the receiver takes the IV, appends it to the defined key (assuming it matches) and decrypts the payload using the generated keystream.

Although not yet part of the protocol specification, many 802.11b vendors also support 128-bit RC4 encryption. This requires a 104-bit WEP key (26 character hexadecimal or 13 character ASCII), but uses the same 24-bit IV value. The figure below shows that the 128-bit encrypted implementations from several vendors are interoperable despite the lack of a standard.

As the name indicates, WEP was never intended to be a panacea for wireless security. Instead, it was designed to afford security equivalent to that provided by an unencrypted wired network. Unlike a wired network, to which physical access is limited by access to the building that houses it, wireless networks are potentially accessible to anyone within range with a compatible receiver.

Discussion :

Key Slot	Bridge		Associated Device	
	Transmit?	Key Contents	Transmit?	Key Contents
1	x	12345678901234567890abcdef	-	12345678901234567890abcdef
2	-	09876543210987654321fedcba	x	09876543210987654321fedcba
3	-	not set	-	not set
4	-	not set	-	FEDCBA09876543211234567890

Figure 15 : WEP Key Example

Over here at this table, there are four different keys and the device is broken into two different categories; the bridge and the other associate device. The key content will be of 128-bit. Once any of the key is chosen as the transmit key, then the other device will have to follow the same key. As an example, the bridge's key 1 is selected as the transmit key, the WEP key 1 on the other device must have the exact same key content. Only then both the devices will be authenticated to communicate with each other. On the other hand, the WEP key 4 is set but because it is not selected as the transmit key, WEP key 4 at the bridge does not need to be set at all. There is no form of security in this method. The characters entered in the Key Content column are not case-sensitive.

The WEP key was successfully established in the hotspot that was created for the purpose of prototype. Users have to enter the WEP username and WEP password in order to get connected to the wireless environment. If the users inputs are not the same as the specified key, the user will not be able to surf the network via mobile.

CHAPTER 5

RECOMMENDATION AND CONCLUSION

5.1 Recommendation

RADIUS SERVER (future upgrade)

The Remote Authentication Dial-In User Service (RADIUS) is a client/server security protocol created by Lucent Remote Access. RADIUS is an Internet draft standard protocol. See RFCs 2138 and 2139 for more information on RADIUS.

User profiles are stored in a central location, known as the RADIUS server. RADIUS clients (such as a PortMaster communications server) communicate with the RADIUS server to authenticate users. The server specifies back to the client what the authenticated user is authorized to do. Although the term RADIUS refers to the network protocol that the client and server use to communicate, it is often used to refer to the entire client/server system.

Basic RADIUS Functions

The primary functions of RADIUS are authentication, authorization, and accounting.

- Authentication

RADIUS determines whether users are eligible to receive requested services.

Authentication information is stored in either a local users file or database cache, or accessed from external authentication mechanisms such as a UNIX password file, ActivCard ActivEngine database, or SecurID ACE/Server database.

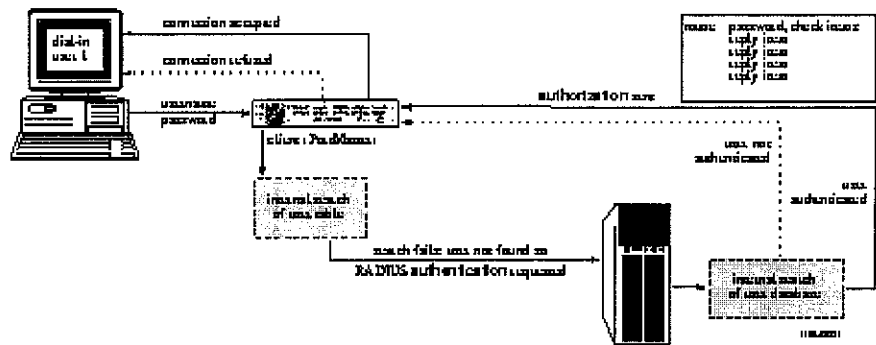


Figure 19 : RADIUS Authentication and Authorization

Procedure of authentication :

1. The PortMaster prompts bob (user) for his username and password, and then compares the username-password pair to the PortMaster user table.
2. The PortMaster sends an access-request message to the RADIUS server if the following conditions are met:
 - Username is not found in the user table
 - Security for the port is set to on
 - RADIUS settings are configured on the PortMaster

The access-request message contains the information necessary for the RADIUS server to authenticate the user.

3. The RADIUS server checks its users file to determine if an entry for user bob is present. For bob's login to be successful, a matching username or DEFAULT entry must be found.

4. User bob is either accepted or rejected:

- If a matching entry is found in the RADIUS users file, if the password requirement is met, and if all check items in the users file are matched by additional attributes in the access-request message, the RADIUS server sends an access-accept message to the PortMaster indicating that bob has been successfully authenticated. It also sends authorization information--reply items--about the services bob can access and configuration information about bob's connection.

-If the password request is not satisfied or if other check items--specified in the RADIUS users file--fail, the RADIUS server sends an access-reject message to the PortMaster indicating that the authentication attempt has failed. The PortMaster terminates bob's connection attempt.

Authorization

Authorization controls access to specific services on the network by configuring the user's session. Once a user is authenticated, RADIUS reports to the PortMaster what a user is authorized (permitted) to access. For example, user bob might be authorized to use the Point-to-Point Protocol (PPP) for his connection, be assigned IP address 192.168.200.4, and have to filter his traffic using packet filters std.ppp.in and std.pp.out .

Accounting

RADIUS accounting stores usage information for dial-in users. This information is often used for billing purposes. When the user is authenticated and the session has been configured according to the authorization information, an accounting start record is created. When the user's session is terminated, an accounting stop record is created.

5.2 Conclusion

Lots of research was done in order to come up with the topic. After gathering some information about hotspot from other educational institutes like KBU and MMU, decided that it was time for UTP to come up with this facility for the students to enable them to be a well rounded person; in the aspect of academy, co-curriculums and technology as well.

In order to create a hotspot in UTP, a lot of issues have to be considered. The most important of crucial decision will be the security of the environment. Since it is wireless, the chances of the data integrity to be violated is very high. Anyone will be able to access the network so proper protection should be given to the network to avoid it from being violated. The very first step taken was to create a authentication method by using WEP for students as well as for the officials in UTP. The username and password has to be specified and accepted by the authentication server before that particular user is given the liberty to access the network.

The second issue of consideration will be cost of the project. As this is an education institute, it is one of their main priorities to keep their students updated with the current technology. Besides, this education institution is along time business and they have to adapt to changes. Hotspot will be very economical because there will not be much cost incurred if in case of expanding the current network. Expansion for current wired environment will be costly because more cables and wires are needed in order to cover the whole campus network. For environment which is wireless, institute will spend way less to accommodate network expansion. So, it will be wiser to have hotspot in campus.

By implementing the hotspot, it is proven that there are advantages of having this wireless environment. Among the advantages that students will gain through this facility will be:

- increase in academic performance
- better team work among students when it comes to group projects
- group studies will be encouraged
- easy access to UTP portal anytime, anywhere within the range of the coverage area to always keep updated about the latest happenings of campus.

There are a few disadvantages when using hotspot as a form of communication with the network. Since hotspot operates purely upon radio waves to transfer data, the weather plays a very important role. If the weather is bad, there will be difficulty in accessing this facility. It will obstruct the radio signals from reaching the user as well as the access point which deals with the data transmission. Secondly since this is hardware based, the tendency for that particular hardware to be stolen is high. Proper protection should be given so that the hardware will be secured from unauthorized people since the hardwares used are costly.

As a conclusion, it is necessary for the management of UTP to provide hotspot in UTP as these technology is in demand by the students. This indirectly can improve the performance of the students as well as the staffs of UTP. This project can be a backbone for future enhancement of hotspots in UTP.

REFERENCES

[1] “Cisco Aironet 350 Series Bridge Software Configuration Guide”, Cisco

a. VLAN Configuration

http://www.cisco.com/en/US/products/hw/wireless/ps458/products_configuration_guide_chapter09186a008007f784.html

b. Configuring Radio and the Basic Settings

http://www.cisco.com/en/US/products/hw/wireless/ps458/products_configuration_guide_chapter09186a008007f77f.html

c. Interface Management

http://www.cisco.com/en/US/products/hw/wireless/ps458/products_configuration_guide_chapter09186a008007f76b.html

d. Security Setup

http://www.cisco.com/en/US/products/hw/wireless/ps458/products_configuration_guide_chapter09186a008007f788.html

[2] “Miltimedia Communications : Application,Networks, Protocols

and Standards”, Fred Halsall,2001,Addison Wesley

[3] www.cisco.com

[4] Wireless – LAN (www.wireless--lan.com) – Wireless LAN sites | WLAN Resources for wireless LAN, WLAN, wireless local area network and WiFi.

[4] Wi-fiplanet (www.wi-fiplanet.com) – Hotspot Hits

[5] wifinetnews (wifinetnews.com)

[6] netserv.du.edu

- a. Denver University – University Technology Services – Network Services
(<http://netserv.du.edu>)
- b. UTS/NS wireless coverage map of Denver University
- c. UTS/NS wireless network

[7] 10meters (www.10meters.com)

Wireless News : Starbucks serving up wireless web access

[8] freewebs (www.freewebs.com)

Wireless LAN| WLAN resource sites

APPENDICES

1.0 Questionnaire

HOTSPOT IN UTP

1. Do you own a computer or laptop or PDA?
 - Yes
 - No

2. Do you use the network often?
 - Yes
 - No

3. Is the connection speed satisfying?
 - Yes
 - No

4. Do you have group meeting in cafes or library after office hours (5 pm onwards)?
 - Yes
 - No

5. Do you think it necessary to have 24 hours network access in these places especially cafes and library?
 - Yes
 - No

6. Will having a wireless network connection in cafes, lecture hall areas and library help in your group meetings?
 - Yes
 - No

7. If wireless technology is implemented in campus, will it allow you to work more efficiently?
 - Yes
 - No

8. Do you think you'll buy a wireless network card to enjoy the wireless facility?

- Yes
- No

9. Would you strongly recommend for the implementation of this wireless technology in UTP especially in cafes, library and lecture hall areas?

- Yes
- No

2.0 Network Diagnostic Page

2.1 Main Page

This page provides access to radio diagnostic tests and provides links to the VLAN Summary Status and SSID statistics pages for access point radios.

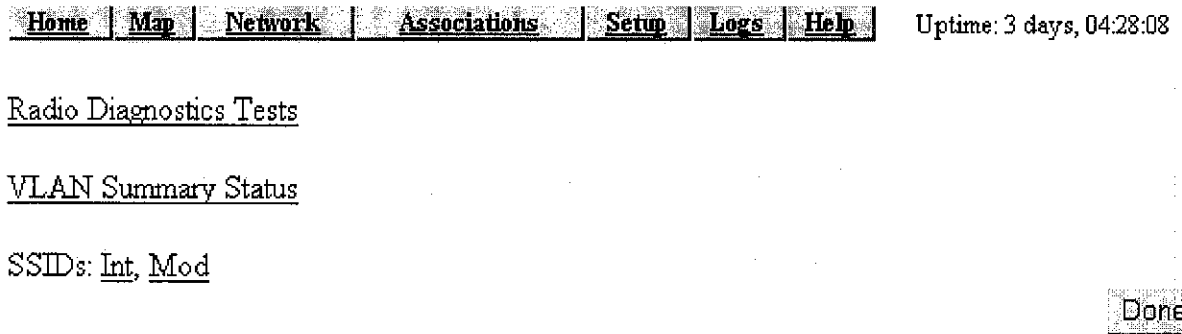


Figure 1 : Main Page

2.1 Radio Diagnostics Tests



Figure 2 : Diagnosis Page

The carrier test measures the amount of radio activity on each frequency available to the access point. Use the carrier test to determine the best frequency for the access point to use. When you conduct a carrier test, make sure all wireless networking devices within range of the access point are operating to make the test results reflect a realistic radio environment.

Carrier Test

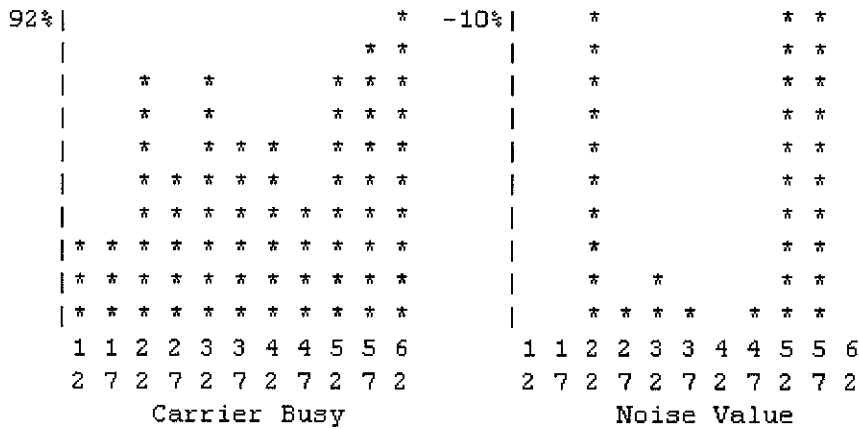


Figure 3 : Carrier Test Window

The bar graph on the left side of the window displays the percentage used for each frequency; the highest current percentage used is labeled on the top left of the graph. In this example, the highest percentage used for any frequency is 92. The access point's available frequencies are listed vertically across the bottom of the graph, from 2412 to 2462 GHz. The access point's channel 1 is 2412 GHz, channel 2 is 2417 GHz, and so on up to channel 11, which is 2462 GHz.

The bar graph on the right side of the window displays the amount of noise on each frequency. Noise is a measurement of the signal the radio receives when it is not receiving packets. Even in an environment in which the radio receives a great deal of noise, it might also receive a strong data signal. Click **Stop Test** in the window or on the Radio Diagnostics page to stop the test.

2.2 Network Port (VLAN Summary Status)

Network Diagnostics

Home Map Network Associations Setup Logs Help			
			Uptime: 4 days, 23:27:31
Name	Ethernet*	Root Radio	Bridge:BR350 West
Status	Up	Up	Up
Max. Mb/s	100.0	11.0	11.0
IP Addr.	10.84.137.71	10.84.137.71	10.84.137.71
MAC Addr.	00409631535e	00409631535e	00409631535e
Radio SSID		bridge	
Receive			
unicast pkts.	33477	1043	114
multicast pkts.	948580	0	589
total bytes	48992558	156555	131190
errors	0	0	0
discards	0	0	0
forwardable pkts.	132981	39171	130
filtered pkts.	0	1303	0
Transmit			
unicast pkts.	45653	1073	117
multicast pkts.	438983	213	773
total bytes	37949231	288969	93564
errors	0	18	0
discards	0	0	0
forwarded pkts.	524980	51601	240

58611

Figure 4 : Network Port Page

Identifying Information and Status

- *Name*—Displays the name of the network interface port. An asterisk (*) next to the name identifies the port as the primary port for the access point.
- *Status*—Displays one of three possible operating states for the port:
 - Up—The port is operating properly.
 - Down—The port is not operating.
 - Error—The port is operating but is in an error condition.

- *Max. Mb/s*—The maximum rate of data transmission in megabits per second.
- *IP Address*—The IP address for the port. When the access point is set up in standby mode the Ethernet and radio ports use different IP addresses. Use the AP Radio Identification page to assign an IP address to the radio port that is different from the Ethernet IP address.
- *MAC (Media Access Control) Address*—The Media Access Control (MAC) address is a unique identifier assigned to the network interface by the manufacturer.
- *Radio SSID*—A unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity.

Data Received

- *Unicast pkts.*—The number of packets received in point-to-point communication.
- *Multicast pkts.*—The number of packets received that were sent as a transmission to a set of nodes.
- *Total bytes*—The total number of bytes received.
- *Errors*—The number of packets determined to be in error.
- *Discards*—The number of packets discarded by the access point due to errors or network congestion.
- *Forwardable pkts.*—The number of packets received by the port that was acceptable or passable through the filters.
- *Filtered pkts.*—The number of packets that were stopped or screened by the filters set up on the port.

Data Transmitted

- *Unicast pkts.*—The number of packets transmitted in point-to-point communication.

- *Multicast pkts.*—The number of packets transmitted that were sent as a transmission to a set of nodes.
- *Total bytes*—Total number of bytes transmitted from the port.
- *Errors*—The number of packets determined to be in error.
- *Discards*—The number of packets discarded by the access point due to errors or network congestion.
- *Forwarded pkts.*—The number of packets transmitted by the port that was acceptable or passable through the filters.

2.3 Ethernet Port

Name		IP	Network	Associations	State	Link	Rel.	Uptime: 03:22:51
Configuration					Set Properties			
Status of "Fast"		Up (Primary)		Maximum Rate (Mb/s)				10.0
IP Address		172.16.24.0		MAC Address				00406623854d
Duplex		Full						
Statistics								
Receive					Transmit			
Unicast Packets		4630		Unicast Packets				3910
Multicast Packets		9330		Multicast Packets				1193
Total Bytes		13867382		Total Bytes				1238105
Total Errors		0		Total Errors				0
Discarded Packets		0		Discarded Packets				0
Forwardable Packets		103199		Forwarded Packets				3379
Filtered Packets		0						
Errors								
Packet CRC Errors		0		Max Retry Packets				0
Carrier Sense Lost		0		Total Collisions				0
Late Collisions		0		Late Collisions				0
Overrun Packets		0		Undersize Packets				0
Packets Too Long		0						
Packets Too Short		0						
Packets Truncated		0						

Figure 5 : Ethernet Port Page

Configuration Information

- The top row of the Configuration section of the table contains a Set Properties link that leads to the Ethernet Hardware page.

- *Status of "fec0"*— "Fast Ethernet Controller" is part of Motorola's naming convention for the Ethernet device used by the access point. This field displays one of the three possible operating states for the port. The added term "primary" identifies the port as the primary port for the access point. Operating states include:
 - Up—The port is operating properly.
 - Down—The port is not operating.
 - Error—The port is in an error condition.
- *Maximum Rate (Mb/s)*—Maximum rate of data transmission in megabits per second.
- *IP Address*—The IP address of the port.
- *MAC Address*—The unique identifier assigned to the access point by the manufacturer.
- *Duplex*—The port's duplex setting, either half or full.

Receive Statistics

- *Unicast Packets*—The number of packets received in point-to-point communication.
- *Multicast Packets*—The number of packets received that were sent as a transmission to a set of nodes.
- *Total Bytes*—Total number of bytes received.
- *Total Errors*—Total number of packets determined to be in error.
- *Discarded Packets*—Packets discarded due to errors or network congestion.
- *Forwardable Packets*—Packets received by the port that were acceptable or passable through the filters.
- *Filtered Packets*—Packets that were stopped or screened by the filters set up on the port.
- *Packet CRC Errors*—Cyclic redundancy check (CRC) errors that were detected in a received packet.
- *Carrier Sense Lost*—The number of disconnects from the Ethernet network. Carrier sense lost events are usually caused by disconnected wiring.

- *Late Collisions*—Packet errors that probably were caused by over-long wiring problems. Late collisions could also indicate a failing NIC card.
- *Overrun Packets*—Ethernet packets that were discarded because the access point had a temporary overload of packets to handle.
- *Packets Too Long*—Ethernet packets that were larger than the maximum packet size of 1518 bytes.
- *Packets Too Short*—Ethernet packets that were shorter than the minimum packet size of 64 bytes.
- *Packets Truncated*—Corrupt or incomplete packets.

Transmit Statistics

- *Unicast Packets*—The number of packets transmitted in point-to-point communication.
- *Multicast Packets*—The number of packets transmitted that were sent as a transmission to a set of nodes.
- *Total Bytes*—Total number of bytes transmitted from the port.
- *Total Errors*—The number of packets determined to be in error.
- *Discarded Packets*—The number of packets discarded by the access point due to errors or network congestion.
- *Forwarded Packets*—The number of packets transmitted by the port that were acceptable or passable through the filters.
- *Max Retry Packets*—Packets which failed after being retried several times.
- *Total Collisions*—The number of packet collisions that occurred through this port.
- *Late Collisions*—Packet errors that were likely caused by overlong wiring problems. Could also indicate a failing NIC card.
- *Underrun Packets*—Packets failed to be sent because the access point was unable to keep up with the Ethernet controller.

2.4 AP Radio Port

Home Map Network Associations Status Logs Help				Uptime: 3 days, 16:21:30	
Options: Detailed Config <input type="checkbox"/> Detailed Stats <input type="checkbox"/> Individual Rates <input type="checkbox"/>				Apply	
Configuration				Set Properties	
Status of "awc0"	Up	Maximum Rate (Mbps)	11.0		
IP Address	10.0.0.1	MAC Address	00029a36421d		
SSID	Test AP 3				
Operational Rates (Mbps)	1.0G, 2.0G, 5.5G, 11.0G	Transmit Power (mW)	100		
Statistics				Refresh	
Receive		Alert <input type="checkbox"/>	Transmit		Alert <input type="checkbox"/>
Unicast Packets		3320	Unicast Packets		35535
Multicast Packets		0	Multicast Packets		31371
Total Bytes		3401551	Total Bytes		16870368
Total Errors		1	Total Errors		2
Discarded Packets		1	Discarded Packets		0
Forwardable Packets		29088	by CoS (0-7):	0, 0, 0, 0, 0, 0, 0, 0	
Filtered Packets		0	Forwarded Packets		70382
Packet CRC Errors		3119453	Max Retry Packets		2
Packet WEP Errors		0	Total Retries		4341
Overrun Packets		0	Cancelled Assoc. Lost		0
Duplicate Packets		1236	Cancelled AID		10
Lifetime Exceeded		0	Lifetime Exceeded		0
MIC Packets		0	MIC Packets		0
MIC Errors		0	MIC Errors		0
MIC Sequ. Errors		0			
MIC Auth. Errors		0			

Figure 6 : Radio Port Page

Configuration Information

- The top row of the Configuration section of the table contains a Set Properties link that leads to the AP Radio Hardware page.
- *Status of "awc0"*—awc0 (Aironet Wireless Communications) is part of Cisco Aironet's naming convention for this radio. This field displays one of three possible operating states:
 - Up—The port is operating properly.
 - Down—The port is not operating.
 - Error—The port is in an error condition.
- *Maximum Rate (Mbps)*—Maximum rate of data transmission in megabits per second. Data rates set to basic are followed by B.
- *IP Address*—The IP address of the radio port.
- *MAC (Media Access Control) Address*—A unique identifier assigned to the network interface by the manufacturer.

- *SSID*—The unique identifier that client devices use to associate with the access point radio. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity.
- *Operational Rates*—The data transmission rates supported and enabled by the access point for communication with client devices.
- *Transmit Power (mW)*—The power level of radio transmission. You can reduce the transmit power to conserve power or reduce interference. Click **Set Properties** to display the AP Radio Hardware page, where you can change this setting.

Receive Statistics

- *Unicast Packets*—The number of packets received in point-to-point communication.
- *Multicast Packets*—The number of packets received that were sent as a transmission to a set of nodes.
- *Total Bytes*—The total number of bytes received.
- *Total Errors*—The total number of packets determined to be in error.
- *Discarded Packets*—Packets discarded due to errors or network congestion.
- *Forwardable Packets*—Packets received by the port that were acceptable or passable through the filters.
- *Filtered Packets*—Packets that were stopped or screened by the filters set up on the port.
- *Packet CRC Errors*—Cyclic redundancy check (CRC) errors that were detected in a received packet.
- *Packet WEP Errors*—Encryption errors received through this port.
- *Overrun Packets*—Packets that were discarded because the access point had a temporary overload of packets to handle.
- *Duplicate Packets*—Packets that were received twice because an acknowledgment was lost and the sender retransmitted the packet.
- *Lifetime Exceeded*—Fragmented packets that were dropped because it took too long to get the next fragment.

- *MIC Packets*—Total number of packets received since system startup and for which a MIC has been requested to be validated with the MMH algorithm.
- *MIC Errors*—Total number of packets received since system startup that failed MIC validation with the MMH algorithm.
- *MIC Sequ. Errors*—Total number of packets received since system startup that failed MIC validation with the MMH algorithm specifically due to sequence number and duplicate packet errors.
- *MIC Auth. Errors*—Total number of packets received since system startup that failed MIC validation with the MMH algorithm specifically due to cryptographic key-mismatch errors.

Transmit Statistics

- *Unicast Packets*—The number of packets transmitted in point-to-point communication.
- *Multicast Packets*—The number of packets transmitted that were sent as a transmission to a set of nodes.
- *Total Bytes*—The number of bytes transmitted from the port.
- *Total Errors*—The number of packets determined to be in error.
- *Discarded Packets*—The number of packets discarded by the access point due to errors or network congestion.
- *Forwarded Packets*—The number of packets transmitted by the port that were acceptable or passable through the filters.
- *Max Retry Packets*—The number of times request to send (RTS) reached the maximum retry number. Click **Set Properties** to display the AP Radio Hardware page, where you can set the maximum RTS value.
- *Total Retries*—The total number of retries that occurred through the radio port.
- *Canceled Assoc. Lost*—Packets dropped because a client device lost association with the access point.
- *Canceled AID*—Packets dropped by a repeater because it roamed to a different parent during a retransmission attempt.

- *Lifetime Exceeded*—Fragmented packets that were dropped because it took too long to deliver a fragment.
- *MIC Packets*—Total number of packets since system startup for which the access point has requested MIC to be calculated with the MMH algorithm before being submitted for transmission.
- *MIC Errors*—Total number of packets which have failed MIC calculation with the MMH algorithm before being submitted for transmission over this radio since system startup.
- *MIC Sequ. Errors*—Packets appear to have arrived either very late or out of sequence. This could be caused by a poor radio link or a replay.
- *MIC Auth. Errors*—The MIC signature is bad due to a calculation with the wrong cryptographic key. These errors could be caused by a simple misconfiguration of a WEP key, or by an attack.

2.5 Event Log

The screenshot shows the Event Log page with the following elements:

- Navigation tabs: Home, Map, Network, Associations, Setup, Logs, Help
- Uptime: 03/26/14
- Index: 0, Number of Events: 10
- Buttons: Next, Prev, Apply New, Purge Log
- Link: Download Event Log
- Text: Press to Change Settings:
- Table with columns: Time, Severity, Description
- Link: additional display filters

Time	Severity	Description
03:26:03	Info	Station Joe Smith Associated
03:26:03	Info	Station Joe Smith Authenticated
03:25:23	Info	Station 209.165.201 Reassociated
03:25:21	Info	Disassociating 209.165.201, reason "Sender is Leaving (has left) BSS"

Figure 7 : Event Log Page

Display Settings

Use the entry fields and the buttons at the top of the page to control the event list. Fields and buttons include:

- Index—Specifies the first event to display in the event list. The most recent event is 0; earlier events are numbered sequentially. To apply your entry, click **Apply New**.
- Number of Events—Specifies the number of events displayed on the page. To apply your entry, click **Apply New**.
- Next—Displays earlier events in the log.
- Prev—Displays more recent events in the log.
- Apply New—Changes the display by applying the settings in the Index and Number of Events fields.
- Purge Log—Permanently deletes all events from the log.
- Additional Display Filters—A link to the Event Display Setup page, where you can change time and severity level settings.

Log Headings

The event log is divided into three columns:

- Time—The time the event occurred. The log records time as cumulative days, hours, and minutes since the access point was turned on, or as wall-clock time if a time server is specified or if the time has been manually set on the access point.
- Severity—Events are classified as one of four severity levels depending on the event's impact on network operations. Severity levels include:
 - Info (green)—Indicates routine information; no error.
 - Warning (blue)—Indicates a potential error condition.
 - Alert (magenta)—Indicates that an event occurred which was pre-selected as something to be recorded in the log. A typical example of an alert would be a packet error condition. The Station page provides check boxes that activate reporting of packet errors to and from the station as alerts in the event log.
 - FATAL (red)—An event which prevents operation of the port or device. For operation to resume, the port or device usually must be reset.