CERTIFICATION OF APPROVAL

WIRELESS LAN IN UTP CAMPUS AREA

by

Rozieyana Binti Rais

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,

Eliza

(Eliza Mazmee Mazlan)

UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK
December 2004

1) Wireless Communication
System

2) IT/IS -- Thesis

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 be undertaken or done by unspecified sources or persons.

ROZIEYANA BINTI RAIS

ABSTRACT

In the world nowadays, more and more organizations and learning institute are deploying the Wireless Local Area Network or WLAN to be used together or to replace with the wired LAN. WLAN is wireless networks between computers within one building or a group of buildings. The frequently used protocol in WLAN is the Wi-Fi (IEEE 802.11 standards. The objective of the project is to develop a conceptual design of a Wireless LAN for UTP campus area. The literature review and case study touch on what is WLAN and its pros such as mobility and the contras such as, the slow network speed and interference. The methodology or steps used to complete the project are project preliminary study, project requirements, project research and analysis, network design and development stage, and lastly the evaluation stage. Though WLAN has some of its downside, it is convenient because of mobility, lower cost to deploy and provide security to its user.

ACKNOWLEDGEMENT

Bismillahirrahmannirrahim...

Firstly, I am grateful to Allah that I am able to finish this project. I would like to thank Universiti Teknologi Petronas (UTP) for giving me the opportunity to gain experience in completing my final year project. I really appreciate all the lessons I have learned throughout my study.

I would also like to express my highest gratitude to all UTP lecturers, especially my supervisor Ms. Eliza Mazmee for her true commitment and guidance throughout the entire development of this project. She has provided such fruitful ideas and recommendations towards completing the project.

My gratitude also goes to Mr. Johari, a consultant at KLCCB, for being very cooperative during our discussion. Not to forget, thank you to Mr. Nizam from Teliti, for giving me the information I needed for this project.

Last but not least, thank you also to all my colleagues, friends and family for their support throughout the project. Thank you.

TABLE OF CONTENTS

APPENDICES

LIST OF FIGURES

ABBREVIATION AND NOMENCLATURES

AP	Access Point
BSA	Basic Service Area
DHCP	Dynamic Host Configuration Protocol
ESA	Extended Service Area
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
PCMCIA	Personal Computer Memory Card International Association
PC	Personal Computer
RF	Radio Frequency
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
UTP	Universiti Teknologi PETRONAS
V1	Village 1
V2	Village 2
V3	Village 3
V4	Village 4
V5	Village 5
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

CHAPTER 1
INTRODUCTION

1.1 Background

Wireless Local Area Network (WLAN), refers to wireless networks between computers within one building or a group of buildings. Two suites of evolving international standards that comprise the core of this course, the IEEE 802.11 (also called WiFi) LAN standard and personal-area networks based on Bluetooth standard, allows enterprises deploy wireless solutions where most productive and without risk. IEEE 802.11b is the most common and established wireless network protocol in use today, referred to as the IEEE 802.11b standard. The 802.11b standard defines, among other things, the radio frequency bandwidth wireless signals can use, throughput rates over that signal, and how wireless endpoints communicate with one another. Well known further WLAN proposal come from the competiting group is Home-RF.

Nowadays, the Wireless LAN is not only deployed by businesses and home users. Many universities; for example, University of Victoria, and a local university; Multimedia University (MMU) Melaka Campus had also deployed the WLAN in their campus area. WLAN will allow campus users to access computing facilities and information sources from portable and mobile computers including hand held devices. The major advantage of WLAN's is mobility.

With Wireless LAN technology, it allows network access without the limitation of wires. However, the performance is not on par with wired technology and security must be actively addressed in the shared wireless environment. In WLAN, wireless access points (base stations) are connected to an Ethernet hub or server and transmit a radio frequency over an area of several hundred to a thousand feet and can penetrate walls and other nonmetal barriers. Roaming users can be handed off from one access point to another like a cellular phone system. Laptops use wireless modems that plug into an existing Ethernet port or that are self contained on PC cards, while standalone desktops and servers use plug-in cards (ISA, PCI, and so on).

1.2 Problem Statement

Currently, UTP campus area is using Local Area Network as a way for campus users to have access to the network. It is only provided in the hostel rooms, offices, library, lecture hall and the laboratory. That means, when the campus users are not in this area, they could not get connected to the Local Area Network, and the Internet. This scenario caused a problem to the campus users, especially the students. The group meetings for example, are always held in the cafeteria, since it is the only venue where the students can freely meet among group members, and have their discussions. Even if the university were to deploy wired LAN in the cafeteria, the idea will seem to be a little comical, since the user's LAN cable laid on the floor (to connect to the hub) will bother the other cafeteria customers. It will also be convenient for the campus users if they could get connected to the network anywhere, at anytime around the campus.

1.3 Objective and scope of study

The objective of this project is to develop a conceptual design of a Wireless LAN for UTP campus area. The research will study the current network design, and determine the areas that need or should be provided with the WLAN, and discover the reasons why that area is more suitable.

Thus, the scope of my project will cover on the best protocol to be used to deploy the Wireless LAN, the coverage areas, how many access points needed, and the network design for the area that will be covered with the WLAN and the security issues regarding the WLAN.

CHAPTER 2
LITERATURE REVIEW

2.1 What is WLAN?

According to Peter J. Welcher and Marty Adkins (2002), WLAN is "the term being used for 802.11-based wireless networks." A WLAN requires a network interface in computer, and the wireless networking device to connect to is a Wireless Access Point (WAP). The WAP may be connected to the other WAPs, but in larger networks, it probably connects to the wired LAN network.

According to John Fisher (2004)

> Wireless LANs (WLANs) utilizes electromagnetic waves, particularly spread-spectrum technology based on radio waves, to transfer information between devices in a limited area." According to him, there are two types of WLAN; infrastructure WLANs and Ad-Hoc WLANs. In an infrastructure WLAN, the wireless network is connected to a wired network such as Ethernet, via access points, which possesses both Ethernet links and antennas to send signals. Devices can communicate with the access points, and through these, with the wired network. For Ad-Hoc WLAN, the users can be connected directly, not by going thru the Access Point first.

Wireless LANs can be as simple as two computers with wireless devices communicating in a peer-to-peer network, or as complex as hundreds or thousands of computers with wireless devices communicating through multiple access points (APs), which bridge network traffic to the wired Ethernet LAN. (Rob Schenk, Andrew Garcia, and Russ Iwanchuk, 2001).

So, in common, they agreed that WLAN involves communication of the computer devices to the AP, that bridge to the wired Ethernet LAN.

2.2 Case Study: WLAN - Advantages and Disadvantages

Louis Stone-Collonge (1998) wrote that: "When the city of Walnut Creek, Calif., needed to interconnect its various LANs dispersed throughout downtown, wireless equipment immediately presented itself. Wireless equipment based on infrared technology was installed atop City Hall and the City Attorney's office across the street. The equipment shot a beam from one rooftop to the other, establishing a 1.5Mbps connection between the two networks--when the equipment worked, that is. The wireless LAN connection was riddled with problems, says Gary Lech, IS manager for the city. The system was so sensitive that trucks passing between the two buildings could throw off the alignment of the infrared equipment, breaking the network connection between the two networks. Heavy fog would also disrupt the connection, as would local wildlife." Pigeons would walk by the equipment [on the roof] and the beam would go out," Lech says. "It was a comedy of errors."

Working with a local VAR, Lech agreed to test RadioLAN Inc.'s CampusLAN wireless equipment. Like the infrared-based equipment, the CampusLAN device established line-of-sight LAN interconnections. Buildings in the campus can be as much as 1,000 feet apart and be connected at 10Mbps. But unlike the infrared-based equipment, it is not based on infrared technology, which had become an untenable solution after the city of Walnut Creek's disastrous experiences. CampusLAN carries data over radio waves, which cannot be disrupted by local traffic, weather conditions, or rooftop wildlife.

A 56Kbps leased line had already replaced the infrared connection between City Hall and the City Attorney's office. So Lech decided to use the RadioLAN devices to interconnect LANs at City Hall and the Regional Center of the Arts, one block away. Antennae were attached to the roofs of the two buildings, and holes drilled into the ceilings for the equipment's conduits. Then the RadioLAN devices were bridged into each building's Ethernet LAN.

In addition to the cost savings, Lech says the radio-based infrastructure is more reliable than the infrared equipment. "There has been no unexpected down time whatsoever" after three months of continuous use, he says. In addition, maintenance of the CampusLink hardware is effortless, according to Lech. "There is no maintenance required. It is unlike a PC or even a router in that regard--it's completely plug-and-play. Once it is configured you can simply forget about it," he says.

A standard wire-based Ethernet infrastructure provides a better upgrade path in terms of bandwidth. Standards-based wireless equipment can only operate at 1Mbps to 2Mbps speeds; RadioLAN's proprietary technology operates at 10Mbps.For a clear migration path to 100Mbps and gigabit speeds, wire-based systems are still the best choice, he says. Though it may not be able to match the speeds of fast Ethernet and gigabit Ethernet, wireless LAN equipment is proving acceptable alternative to slow and expensive leased lines in an extended campus environment."

From this case, though the WLAN is slower than the wired network, it is cost-saving and easier to deploy since it does not involves tearing up the streets to lay the cables, if the wired network were to be used. By using the radio wave that cannot be disrupted by local traffic, weather conditions, or rooftop wildlife, instead of infrared, the interference could be reduced.

Meanwhile, according to Josh Fisher and Rosemary Wang; WR Hambrecht + Co cited that, "WLAN is easier to deploy and configure, more secure, ultimately more cost-effective (scalable), facilitates office relocation (network portability), easier to maintain, and makes available real-time data in broader range of coverage areas. " But, it comes with a few disadvantages too. The disadvantages of deploying WLAN are; "the slower network speed, and the signal interference often causes disruptions in connection, and systems from different vendors may not be interoperable. The costly installation is also one of the cons of using WLAN. "(John Fisher and Rosemary Wang)

In addition to increased mobility, wireless LANs offer increased flexibility. It is more economical to use a wireless LAN. Wireless LANs offer the connectivity and the convenience of wired LANs without the need for expensive wiring or rewiring. (Daniel L. Lough, T. Keith Blankenship, Kevin J. Krizman, 1997)

2.3 Components of WLAN

Components of a WLAN are access points, NICs or client adapters, bridges, and antennas.

- *Access point*—An access point operates within a specific frequency spectrum and uses an 802.11 standard specified modulation technique. It also informs the wireless clients of its availability and authenticates and associates wireless clients to the wireless network. An access point also coordinates the wireless clients' use of wired resources.
- *NIC or client adapter*—A PC or workstation uses a wireless NIC to connect to the wireless network. The NIC scans the available frequency spectrum for connectivity and associates it to an access point or another wireless client. The NIC is coupled to the PC or workstation OS using a software driver.
- *Bridge*—Wireless bridges are used to connect multiple LANs (both wired and wireless) at the Media Access Control (MAC) layer level. Used in building-to-building wireless connections, wireless bridges can cover longer distances than access points (IEEE 802.11 standard specifies 1 mile as the maximum coverage range for an access point).
- *Antenna*—An antenna radiates the modulated signal through the air so that wireless clients can receive it. Characteristics of an antenna are defined by propagation pattern (directional versus omnidirectional), gain, transmit power, and so on. Antenna usually comes with the access point.

2.4 Standard WLAN Design Guidelines

In the standard WLAN designs, it is assumed that all WLAN devices are connected to a unique IP subnet to enable end-user mobility throughout various designs. An assumption is made in the designs that most services available to the wired network are also available to the wireless network addition. All designs should include the following WLAN security principles:

- Access point security recommendations:
  - Enable centralized user authentication (RADIUS, TACACS+) for the management interface.
  - Choose strong community strings for Simple Network Management Protocol (SNMP) and change them often.
  - Consider using SNMP Read Only if your management infrastructure allows it.
  - Disable any insecure and nonessential management protocol provided by the manufacturer.
  - Utilize secure management protocols, such as Secure Shell Protocol (SSH).
  - 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.
- Client security recommendations:
  - Disable ad hoc mode.
  - Enable wireless frame encryption where available.

2.5 Wireless Security Issues

As standardized by the IEEE, security for 802.11 networks can be simplified into two main components: encryption and authentication. The implementation of these components has been proven and documented as insecure by the security community at large.

Frame Encryption

Properly performed encryption allows for confidentiality. Encryption is the process of taking a message, referred to as cleartext, and passing it through a mathematical algorithm to produce what is known as ciphertext. Decryption is the reverse of the process. Encryption algorithms typically rely on a value, called a key, in order to encrypt and decrypt the data. Two major forms of encryption are used today—symmetric encryption (also known as shared-key encryption) and asymmetric encryption (also know as public or private encryption). Symmetric encryption is about 1000 times faster than asymmetric encryption, and is, therefore, used for the bulk encryption of data. Generally with well-designed encryption algorithms, longer keys result in a higher degree of security because more brute force is required to try every possible key (known as the key space) in order to decrypt a message.

The IEEE has specified that wired equivalent privacy (WEP) be the means to encrypt 802.11 data frames. 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. A stream cipher is one that operates the encrypt or decrypt function on a unit of plaintext (in this case, the 802.11b frame). This cipher is contrasted with a block cipher, which processes a fixed number of bytes in each encrypt or decrypt function. With symmetric encryption, the key is the one piece of information that must be shared by both the encrypting and decrypting endpoints. RC4 allows the key length to be variable, up to 256 bytes, as opposed to requiring the key to be fixed at a certain length. IEEE specifies that 802.11 devices must support 40-bit keys, with the option to use longer key lengths. Several vendors support 128-bit WEP encryption with their WLAN solutions.

Because WEP is a stream cipher, a mechanism is required to ensure that the same plaintext will not generate the same ciphertext. The IEEE stipulated the use of an initialization vector to be concatenated with the symmetric key before generating the stream ciphertext.

The initialization vector is a 24-bit value (ranging from 0 to 16777215). The IEEE suggests—but does not mandate—that the initialization vector change per frame. Because the sender generates the initialization vector with no standard scheme or schedule, it must be sent to the receiver unencrypted in the header portion of the 802.11 data frame. The receiver can then concatenate the received initialization vector with the WEP key (base key) it has stored locally to decrypt the data frame. As illustrated in Figure 1, the plaintext itself is not run through the RC4 cipher, but rather the RC4 cipher is used to generate a unique keystream for that particular 802.11 frame using the initialization vector and base key as keying material. The resulting unique keystream is then combined with the plaintext and run through a mathematical function called XOR. This produces the ciphertext.

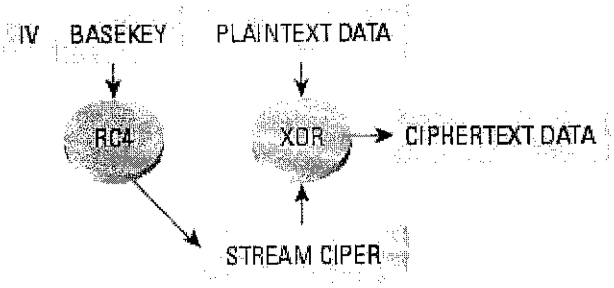


Figure 1: WEP Encryption Process

Authentication Mechanism

The IEEE specified two authentication algorithms for 802.11-based networks. First, open authentication is a null authentication algorithm because any station requesting authentication is granted access. The second form of authentication is called shared-key authentication, which requires that both the requesting and granting stations be configured with matching WEP keys. The requesting stations send an authentication request to the granting station. The granting station sends a plaintext challenge frame to the requesting station. The requesting station WEP encrypts the challenge frame and sends it back to the granting station. The granting station attempts to decrypt the frame, and if the resulting plaintext matches what the granting station originally sent, then the requesting station has a valid key and is granted access.

Note that shared-key authentication has a known flaw in its concept. Because the challenge packet is sent in the clear to the requesting station and the requesting station replies with the encrypted challenge packet, an attacker can derive the stream cipher by analyzing both the plaintext and the ciphertext. This information can be used to build decryption dictionaries for that particular WEP key.

2.6 Network Design and Development

During this network design and development stage, the network design for WLAN in UTP campus is designed and developed. Then, the design will be referred to the network engineer. The pros and cons of the design will be discussed, and if there is anything to be improved on the design, changes will be made to the design.

2.6.1 Types of Network Structure

According to Daniel L. Lough, T. Keith Blankenship, Kevin J. Krizman (1997)

> In IEEE's proposed standard for wireless LANs (IEEE 802.11), there are two different ways to configure a network: ad-hoc and infrastructure. In the ad-hoc network, computers are brought together to form a network "on the fly." As shown in Figure 2, there is no structure to the network; there are no fixed points; and usually every node is able to communicate with every other node. A good example of this is the aforementioned meeting where employees bring laptop computers together to communicate and share design or financial information. Although it seems that order would be difficult to maintain in this type of network, algorithms such as the spokesman election algorithm (SEA) have been designed to "elect" one machine as the

base station (master) of the network with the others being slaves. Another algorithm in ad-hoc network architectures uses a broadcast and flooding method to all other nodes to establish who's who.

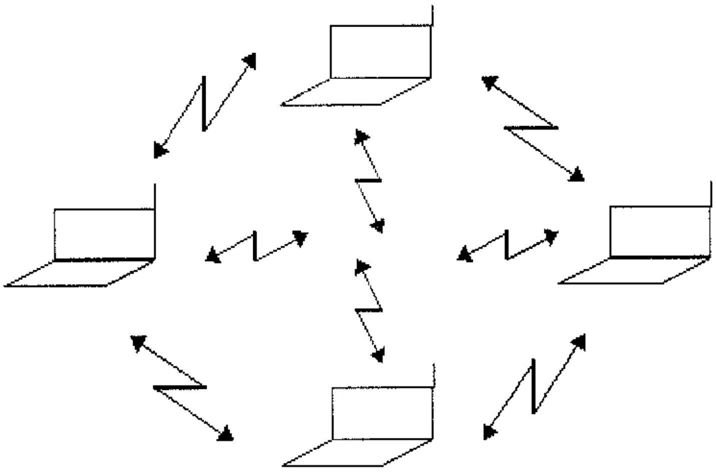


Figure 2: Ad-Hoc Network

As shown in Figure 3, the second type of network structure used in wireless LANs is the infrastructure. This architecture uses fixed network access points with which mobile nodes can communicate. These network access points are sometime connected to landlines to widen the LAN's capability by bridging wireless nodes to other wired nodes. If service areas overlap, handoffs can occur. This structure is very similar to the present day cellular networks around the world. (p.9)

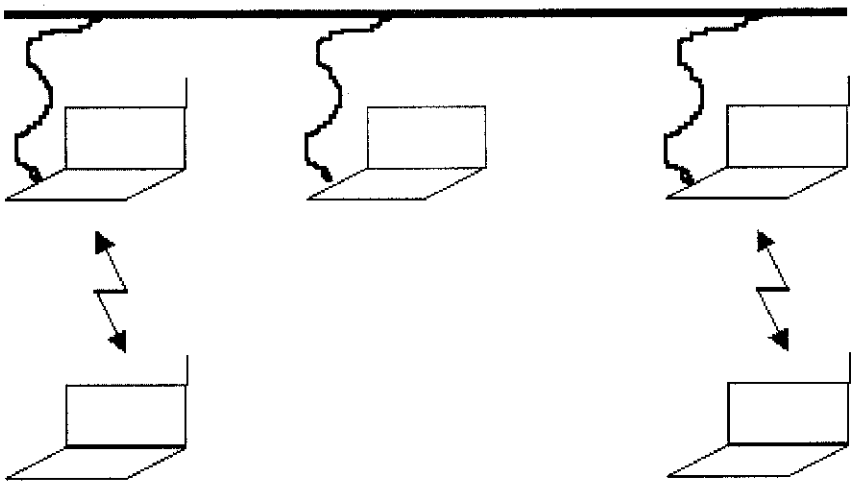


Figure 3: Infrastructure Network

Sean Convery, Darrin Miller and Sri Sundaralingam (2004) seem to agree with the previously mentioned writers.

In general, IEEE 802.11 WLANs typically operate in either of two modes:

- Infrastructure Mode
- Ad-hoc Mode

Infrastructure Mode

In infrastructure mode, clients communicate through an AP. The AP is the point at which wireless clients can access the network. Figure 1-3 illustrates a typical WLAN arrangement. The AP provides connectivity to other clients associated with that AP or to the wired LAN. The basic service area (BSA) is the area of RF coverage provided by an AP—also referred to as a microcell. To extend the BSA, or to simply add wireless devices and extend the range of an existing wired system, an AP can be added.

The AP attaches to the Ethernet backbone and communicates with all the wireless devices in the cell area. The AP is the master for the cell, and controls traffic flow to and from the network. The remote devices do not communicate directly with each other—they communicate to the AP. If a single cell does not provide enough coverage, any number of cells can be added to extend the range. This is known as an extended service area (ESA). It is recommended that the ESA cells include 10-to-15 percent overlap to allow remote users to roam without losing RF connections. Bordering cells should be set to different non-overlapping channels for best performance.

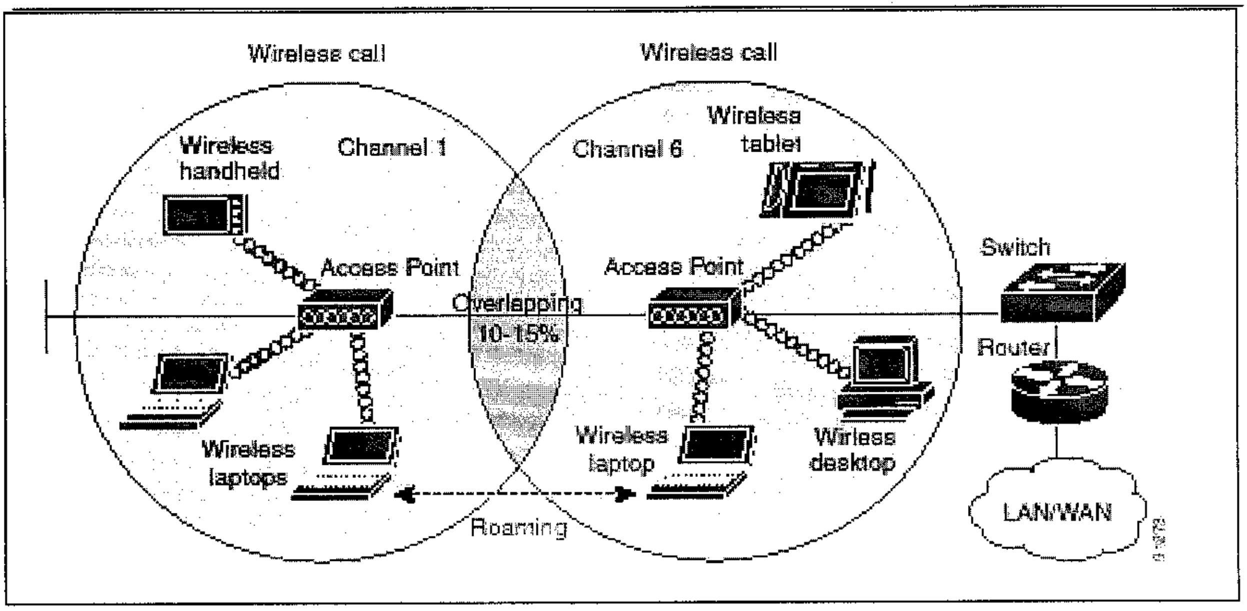


Figure 4: Typical WLAN Design

CHAPTER 3
METHODOLOGY/PROJECT WORK

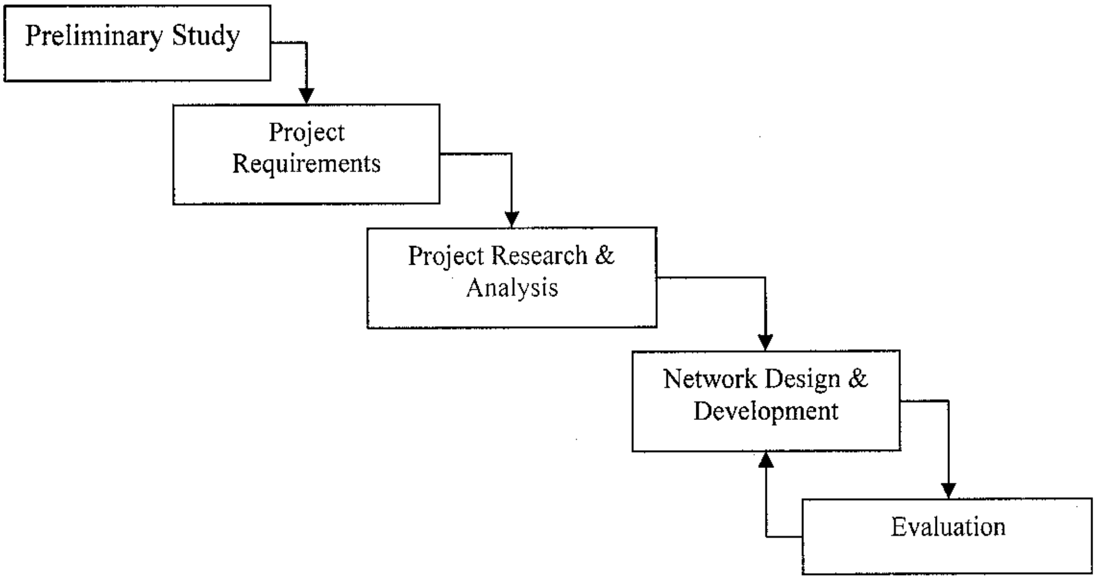


Figure 5: Project Methodology

3.1 Preliminary Study

In this first phase, I have to define problem statement, aim, objective and scope of the project. Then, the proposal for the project is written and sent for approval. Also, I have to plan out the details for the project, as a guideline of the flow of the project. The methodology for the project will be formulated, and the Gantt chart for the project flow will be constructed (refer Appendix 1).

3.2 Project Requirements

This is the second phase where all the research about WLAN is done. The questionnaires (refer to Appendix 2) that are needed for the project is constructed in this stage. It involves giving away questionnaires to the students in UTP campus. The purpose of the questionnaires is to find out the location to be provided with the WLAN. With the questionnaires, the area that the students feel most needed to be provided with WLAN facility will be discovered. The reason why the questionnaires are given to the student is that, the students are the biggest population in the campus. They spend most of their time in the campus, since they live in the campus area.

In this stage also, the tools required for the project will be identified. For drawing network design, there are several software that can be used to draw network design such as LanFlow, Net Diagrammer, Microsoft Visio and SmartDraw. For this project, Microsoft Visio is used to draw the network diagram, and Packet tracer is used to show the simulation.

3.3.1 Project Research & Analysis

In this stage, my work will involve researching from journal and Internet regarding various issues of WLAN. There will also discussions with UTP IT Department and Network Engineer, and interviews (for questions for interview, refer Appendix 3). During this stage also, the important and relevant information from the project research is abstracted. Then, it will be analyzed and the data will be used for the next stage.

3.4 Network Design and development

During this network design and development stage, the network design for WLAN in UTP campus is designed and developed. Then, the design will be referred to the network engineer. The pros and cons of the design will be discussed, and if there is anything to be improved on the design, changes will be made to the design.

3.5 Evaluation

This is the last stage in this project where the evaluation of the network design is done. The design will be referred to the network engineer. The pros and cons of the design will be discussed, and if there is anything needs to be improved on the design, the network design and development stage will be re-visited. Then, changes will be made, and the design will be updated, and improved.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Project Requirements

4.1.1 Results of Questionnaires

According to the questionnaires given to the 100 UTP students, 99% of them have a PC or a laptop (Figure 6). This means, almost about 99% students in UTP may need the LAN facility provided by UTP campus. This is because, all the rooms in residential buildings are equipped with network port, as a mean for the students to get connected to the LAN. Knowing this, the students would likely equipped their PC or laptop with network card (furthermore, almost all motherboard in the market currently have a built-in network card). Meanwhile, 55% of the students view the current LAN services is good, which means, satisfying, and 13% feels that it needs improvement(Figure 7). 59% of the students would like WLAN to be installed in UTP (Figure 8), but it seems that 89% are willing to spend below RM100 to get the facility (Figure 10). Meanwhile, for the location of WLAN service, 61% students agree that the cafeteria is location that needs WLAN the most. Only 5% thinks that WLAN is needed in their room (Figure 9). This may be caused of the existing faster wired LAN in the rooms provided by UTP campus. For the application of WLAN, 44% of the students want to use it for doing research, 30% to access the E-Learning website, and 23% want to access their Emails (Figure 11).

Based on the results of the questionnaires, it is proved that the students of University Technology of PETRONAS are ready for WLAN. This is because, almost all of the students have a personal computer or a laptop. For the location of the WLAN, cafeterias are the most wanted location to be provided with WLAN. This also proves that the students are aware of the wireless technology, and it is good for them to be exposed to it. The wireless equipments are getting more popular nowadays and the price are getting lower too. A common 802.11b wireless PCMCIA card cost about a little over RM100 at the current market. Though not many students are willing to spend more than RM100 for the cost of buying the wireless adapter, deployment of WLAN might be able to change it.

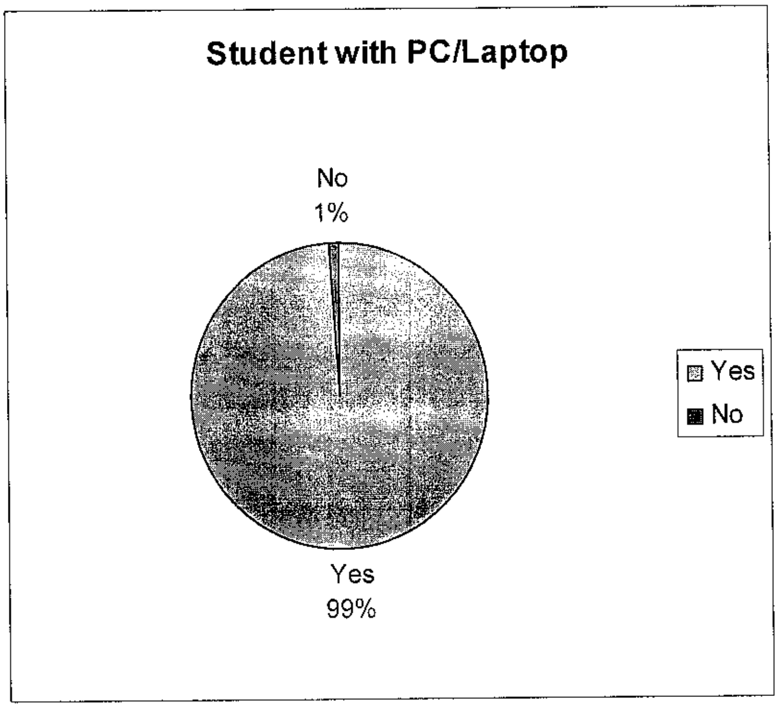


Figure 6: Students with PC/Laptop

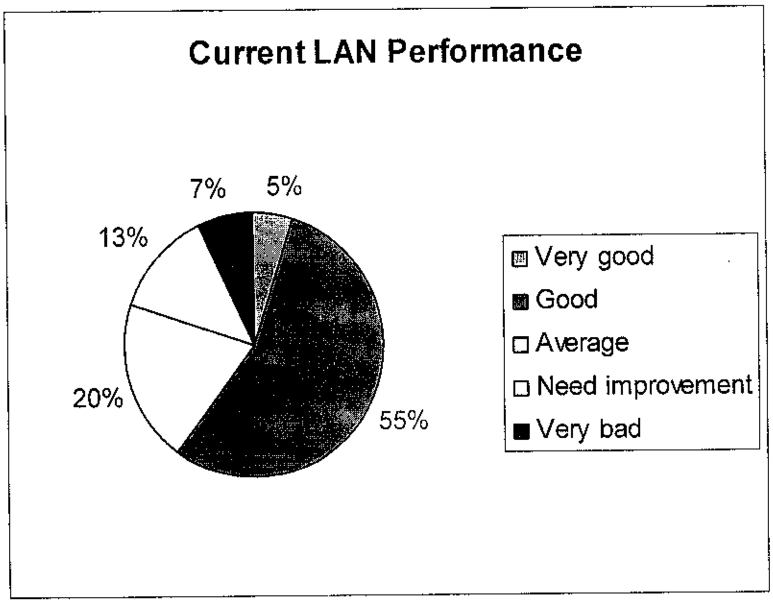


Figure 7: Current LAN Performance

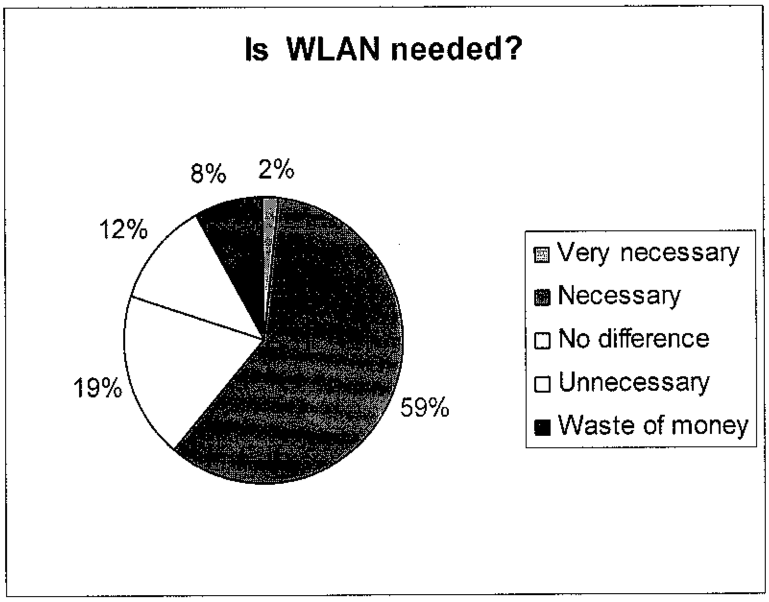


Figure 8: The Need for WLAN

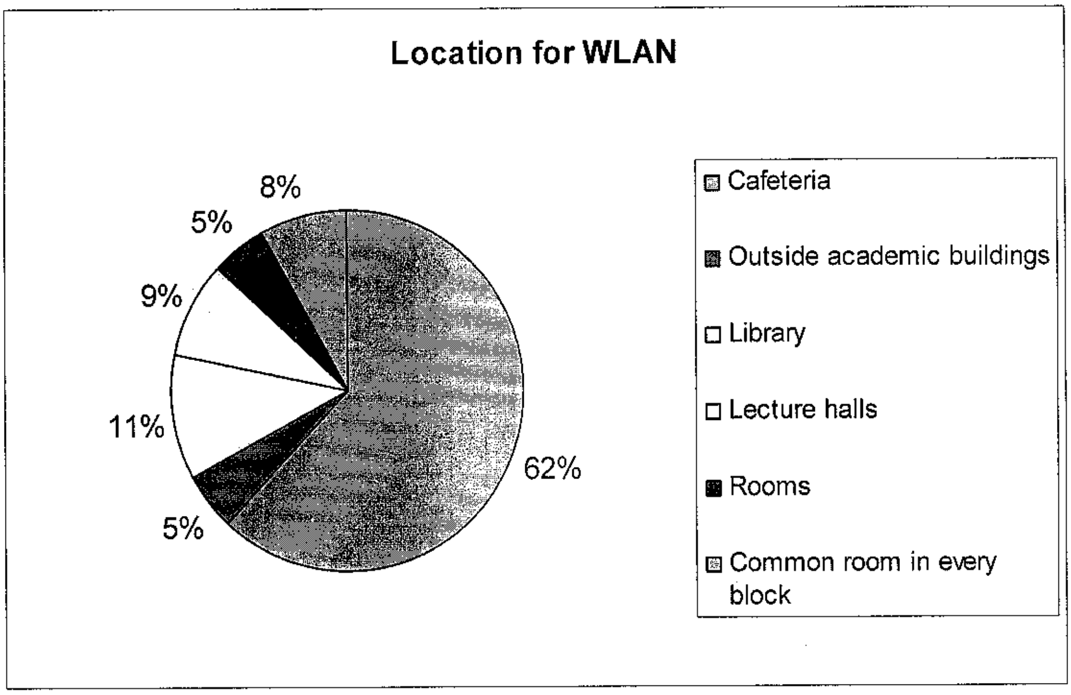


Figure 9: Suitable Locations for WLAN

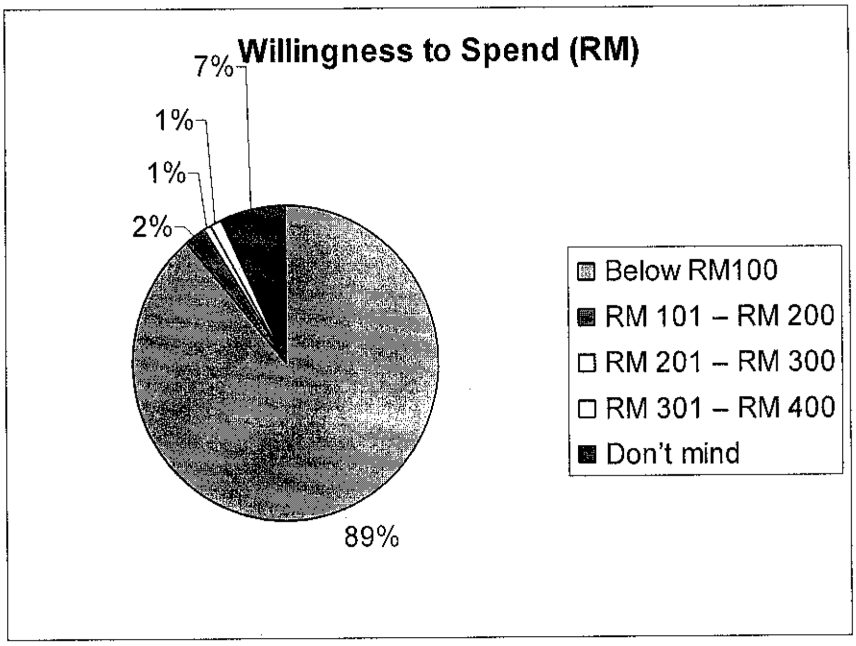


Figure 10: Willingness to Spend on WLAN

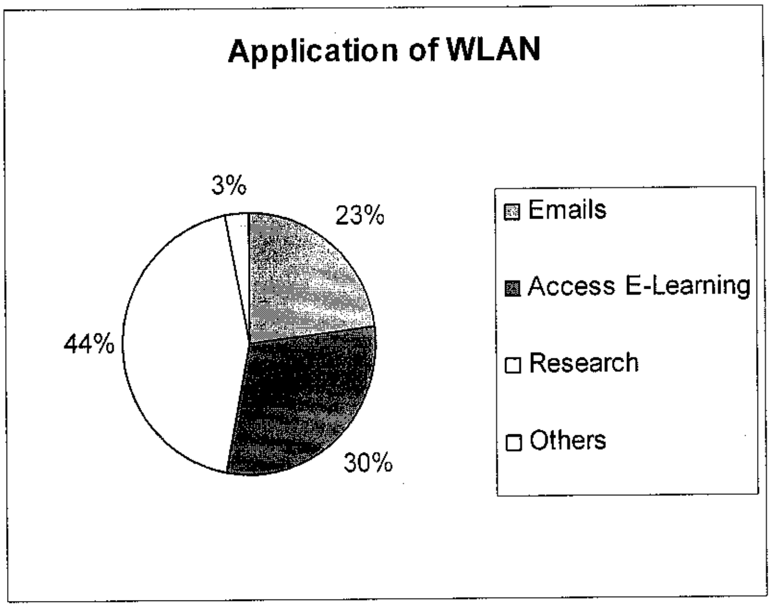


Figure 11: Usage of WLAN

4.2 Project Research & Analysis

4.2.1 UTP Current Setup

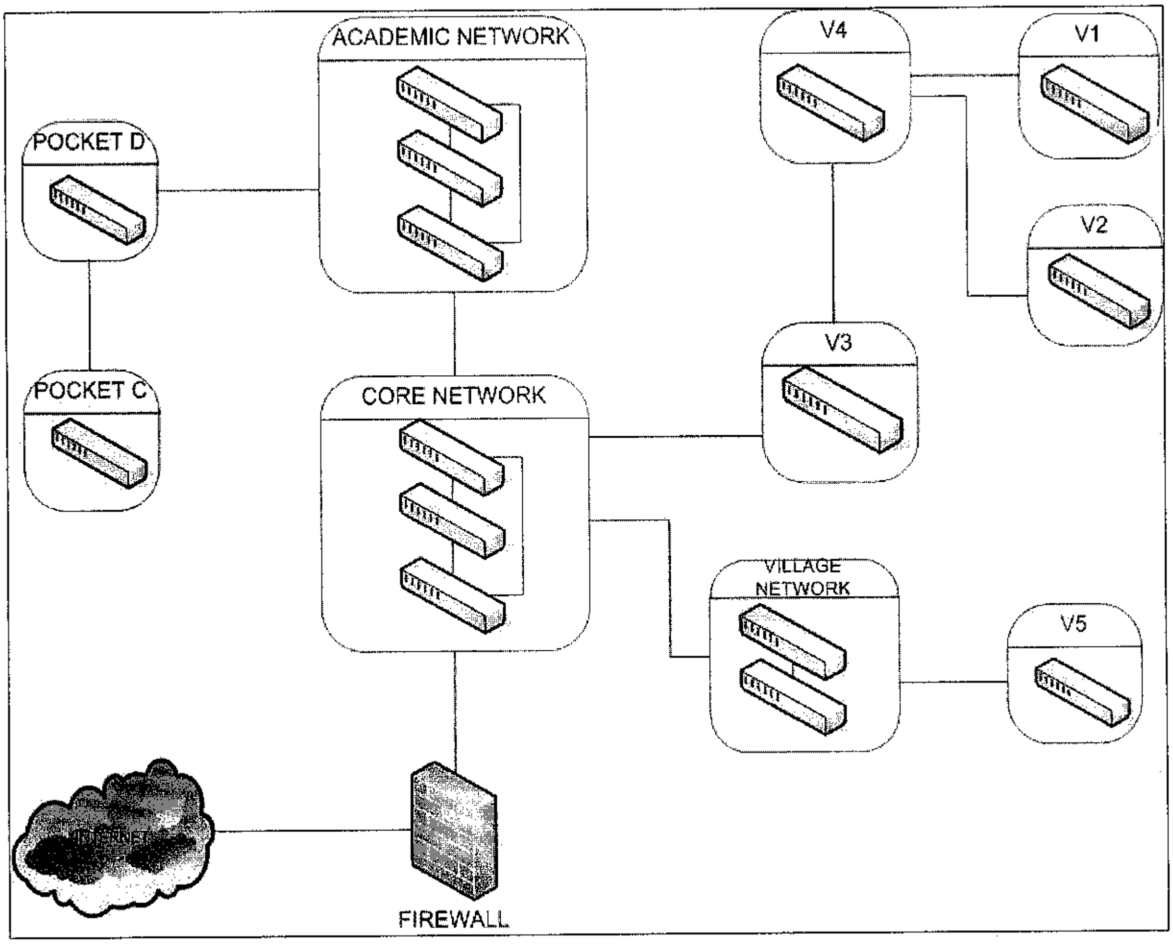


Figure 12: UTP Current Setup

Referring to Figure 12, currently, in the residential area, there are many switches in each of the building block. All the switches are connected to the passport in the Data Centre in the cafeteria area in each village. The entire passport in Village 1 (V1), Village 2 (V2), and Village 4 (V4) are connected then to the passport in Village 3 (V3). Then the passport in V3 will be connected to the core network, at UTP Data Centre. Meanwhile, for Village 5 (V5), the passport is connected to the Village Network passports, and then connected to the core network. For the academic area, the passport in Pocket C is connected to Academic Network before being connected to the core network. But, since the distance from Pocket C and the Data Centre is too far, another passport is placed in Pocket D, to connect to the passport in core network.

4.3 Network Design & Development

4.3.1 Basic Design

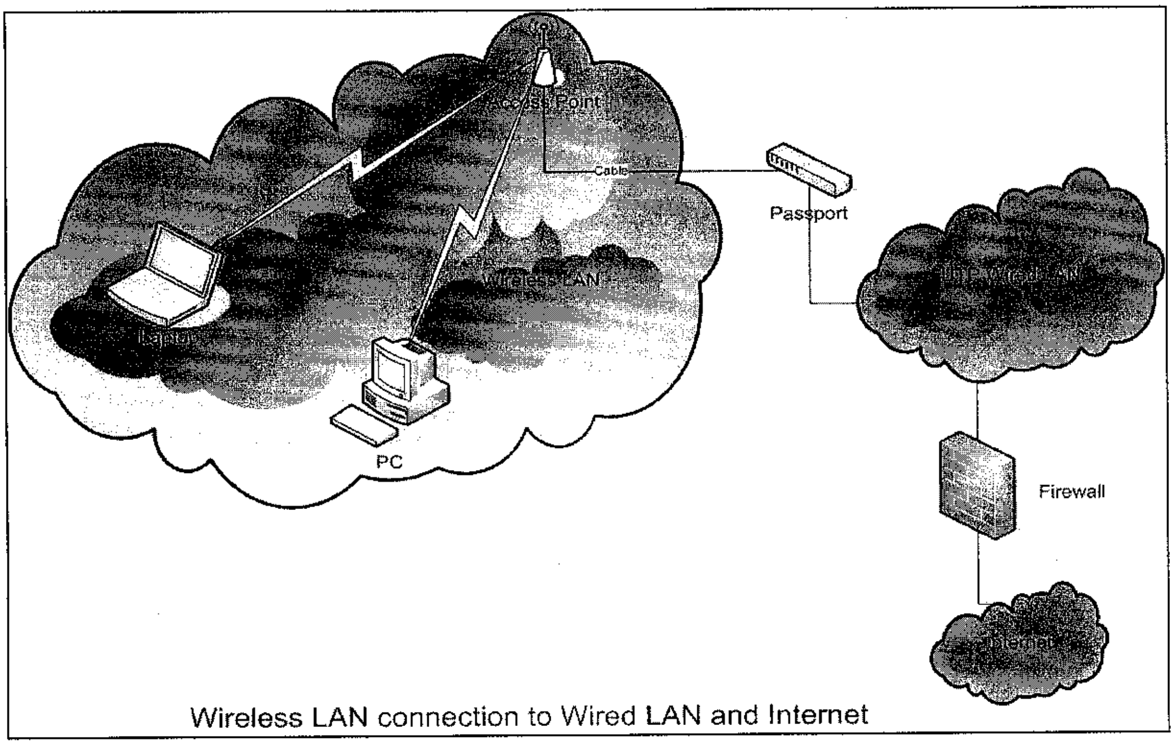


Figure 13: Basic WLAN Design

The diagram above shows the basic WLAN design for UTP current network. An access point will be connected to a passport or a switch, before it is connected to the current existing LAN. The users in the coverage area will get the radiowave signal from the access point, and will be able to connect to the current LAN and the Internet. In order to do that, the user must have an adapter that can detect the wireless signal. Then, the users have to setup the computer/laptop and change it to wireless mode. Next, the users are required to set the Internet Protocol (IP) for the computer/laptop, according to the IP of the area.

4.3.2 Overall Design

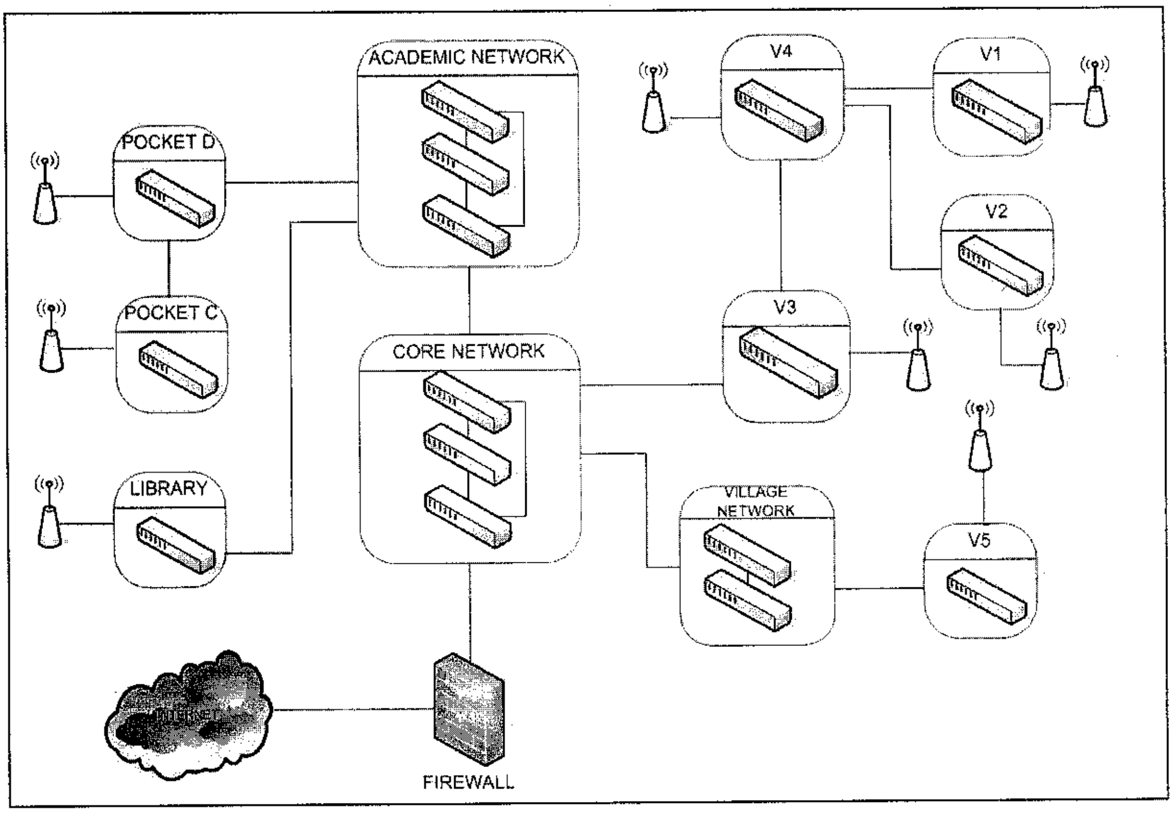


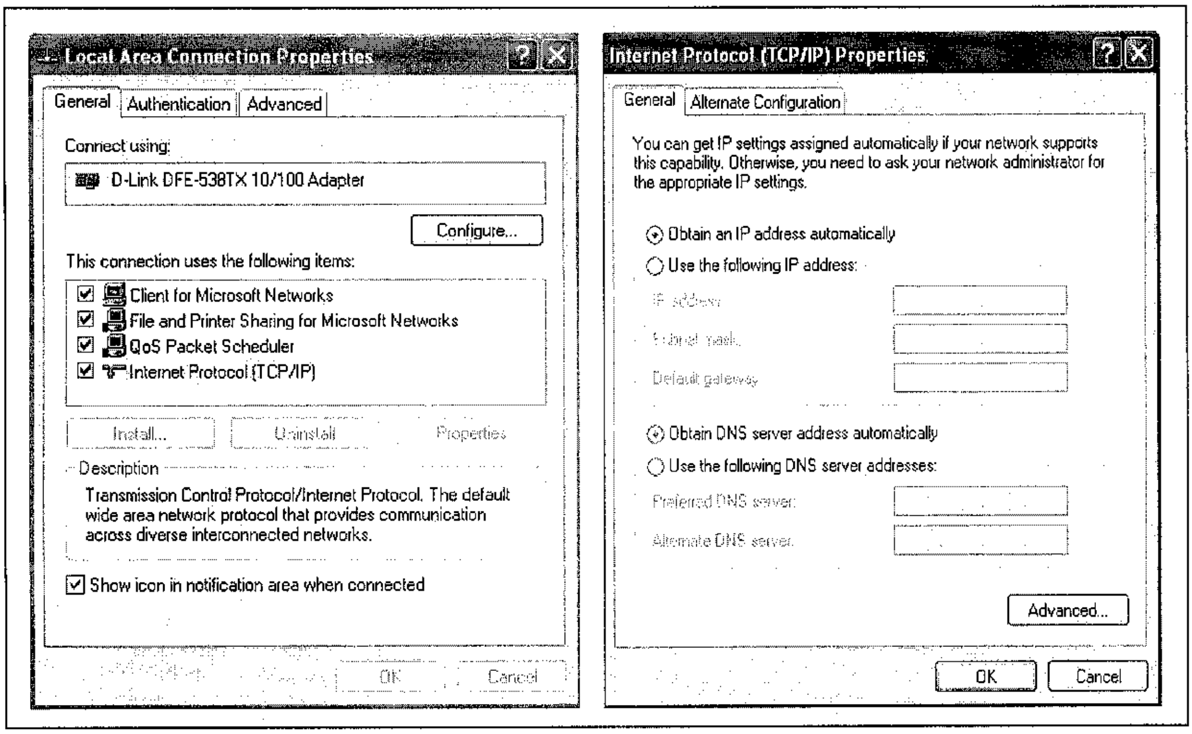
Figure 14: Overall Design

This diagram shows the WLAN overall design. For all the villages (V1, V2, V3, V4, V5), one access point is placed at the café near data centre at each village. The access point will be connected to the passport at each village. The passports in V1, V2, and V4 will be connected to the passport in V3, and then connected to the core network at UTP Data Centre. For V5, the passport will be connected to the Village Network first, then to the core network.

For each village, the access point will be located at the cafeteria, since the cafeteria is the place where the students always gather, and there is no way of getting access to the network there. Furthermore, the cafeteria is the closest area to the village's Data Centre, making it easier to connect the access point to the passport.

The passport in Data Centre of the village is used instead of the switch in the nearest block to the cafeteria is because, more users will be able to get access to the LAN. Since the IP in each block is configured using type C IP, only about 250 users are able to get connected to the network at one time. Currently, about 153 are residing in each block. Thus, only about 100 IP address are free. This means, only about 100 users in the cafeteria are able to get access to the network since they will be using the IP of that residential block. This will be a waste, since an access point that are usually used in area like a campus, can support till 250 users at once.

By using the passport in the Data Centre, a new LAN has to be setup at the passport. This means, a new IP will be assigned, especially for the access point. Then, the access point can be set, whether to use manual or automatic IP address configuration. Since the residential area's IP addresses are configured automatically by DHCP server, it is better to set it the same, so that it will be easier for the students. The students will need to let the DHCP set the IP for their computer/laptop (Figure 15). The student has to set their TCP/IP properties to 'Obtain an IP address automatically' to enable the Dynamic Host Configuration Protocol. This is a protocol that lets network administrators centrally manage and automate the assignment of IP Addresses on the corporate network. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.



Connect using:

D-Link DFE-538TX 10/100 Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

Figure 15: Configuring Automatic IP for Computer/laptop

Currently, for the academic buildings area, the IPs are fixed, and need to be configured manually. This situation will make it difficult for the students to have access to the network since they will need to know the building's IP. To make it easier for them, the AP put in this block should be set to use automatic IP instead. This way, the students can use the automatic IP configuration to gain an IP.

Meanwhile, for this area, there is a passport in Pocket C building. An access point can be connected to the passport in this building to enable the students in this area to get access the network. The passport in the Pocket C is then connected to the passport in Pocket D building. There also, an access point can be connected to the passport so that the students in Pocket D area will be able to get access to the network. The reason why these areas are chosen is that because Pocket C and Pocket D is the location of the lecture rooms. Furthermore, in the future time, there will be cafeterias on these two buildings, making it the gathering centre of the students.

4.3.3 Coverage Area

Originally, the access point used is able to cover about 100m radius. But, 92m is used, for accuracy reason, since it is not possible to get 100% coverage since there are obstacles such as doors, and walls. But, for the library area (Figure 20), the coverage area is smaller compared to the other area, since the library walls are made of glass. This can greatly reduced the signal sent by the access point.

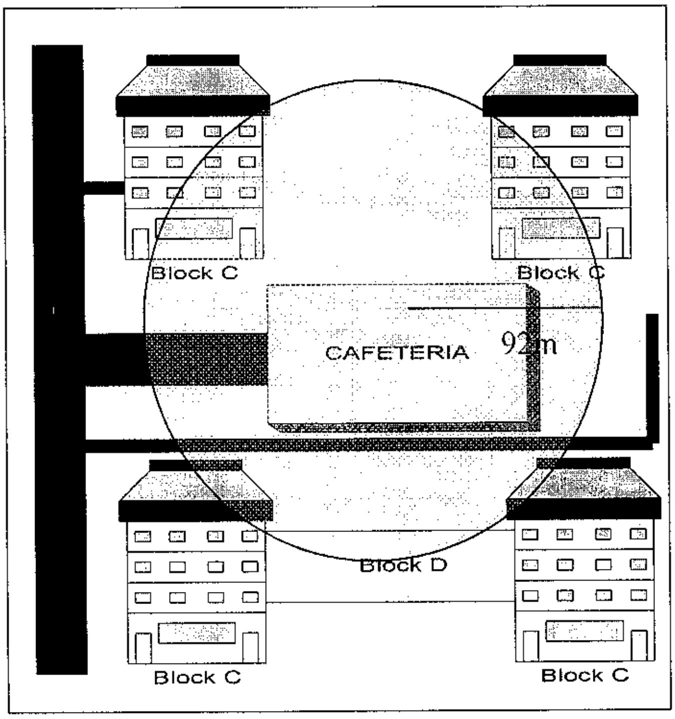


Figure 16: Village 2 (V2) Coverage Area

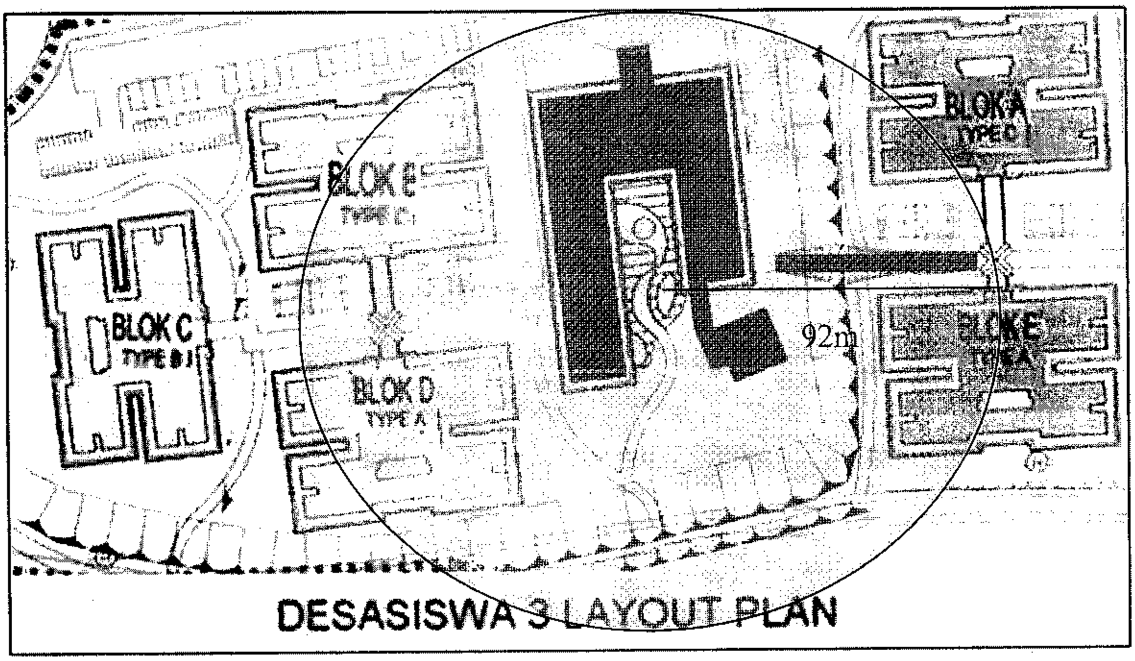


Figure 17: Village 3(V3) Coverage Area

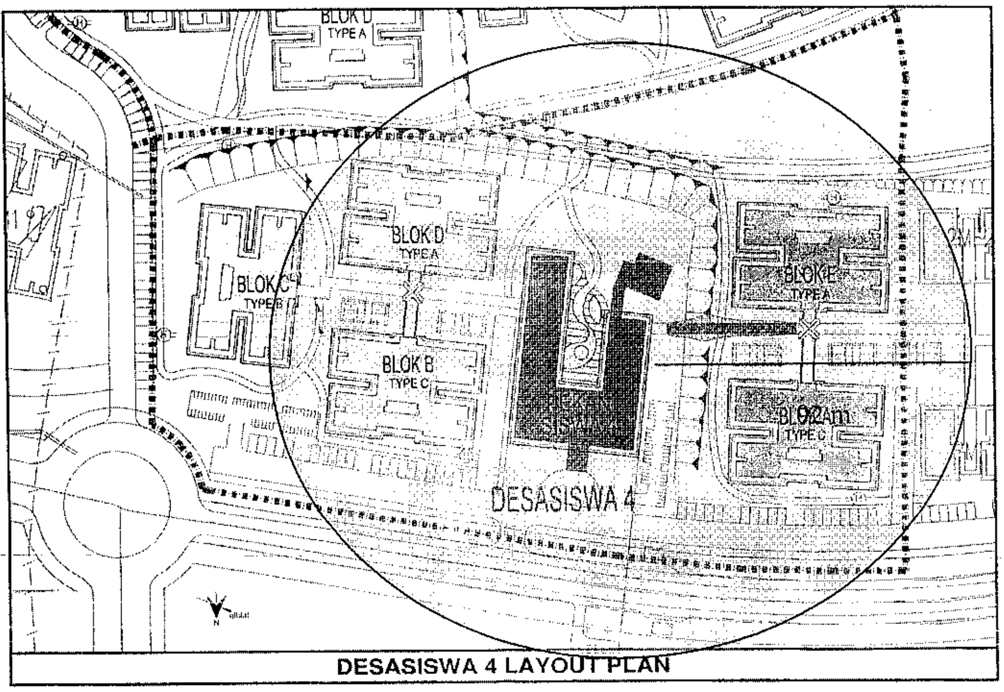


Figure 18: Village 4 (V4) Coverage Area

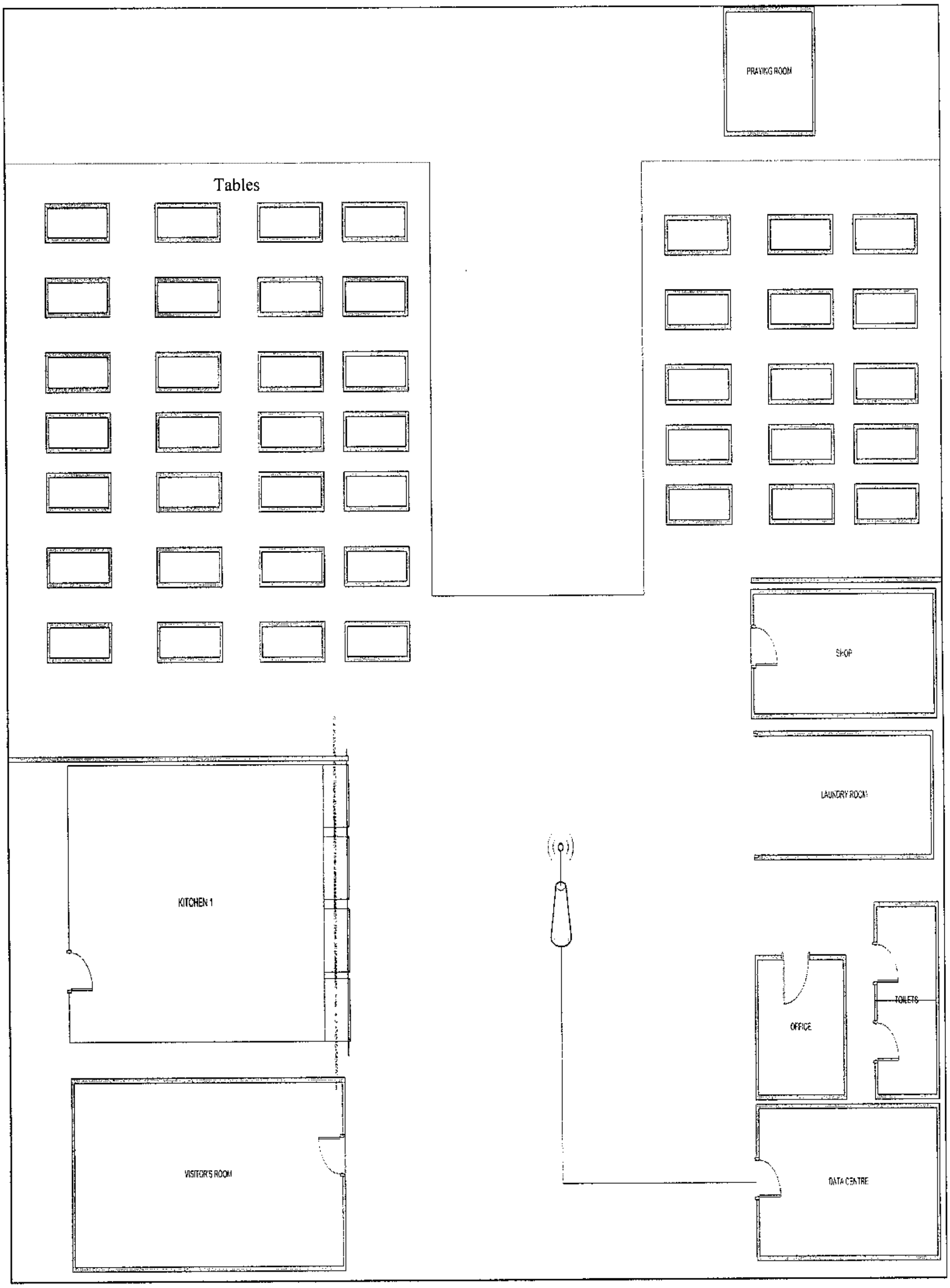


Figure 19: Cafeteria Layout Plan

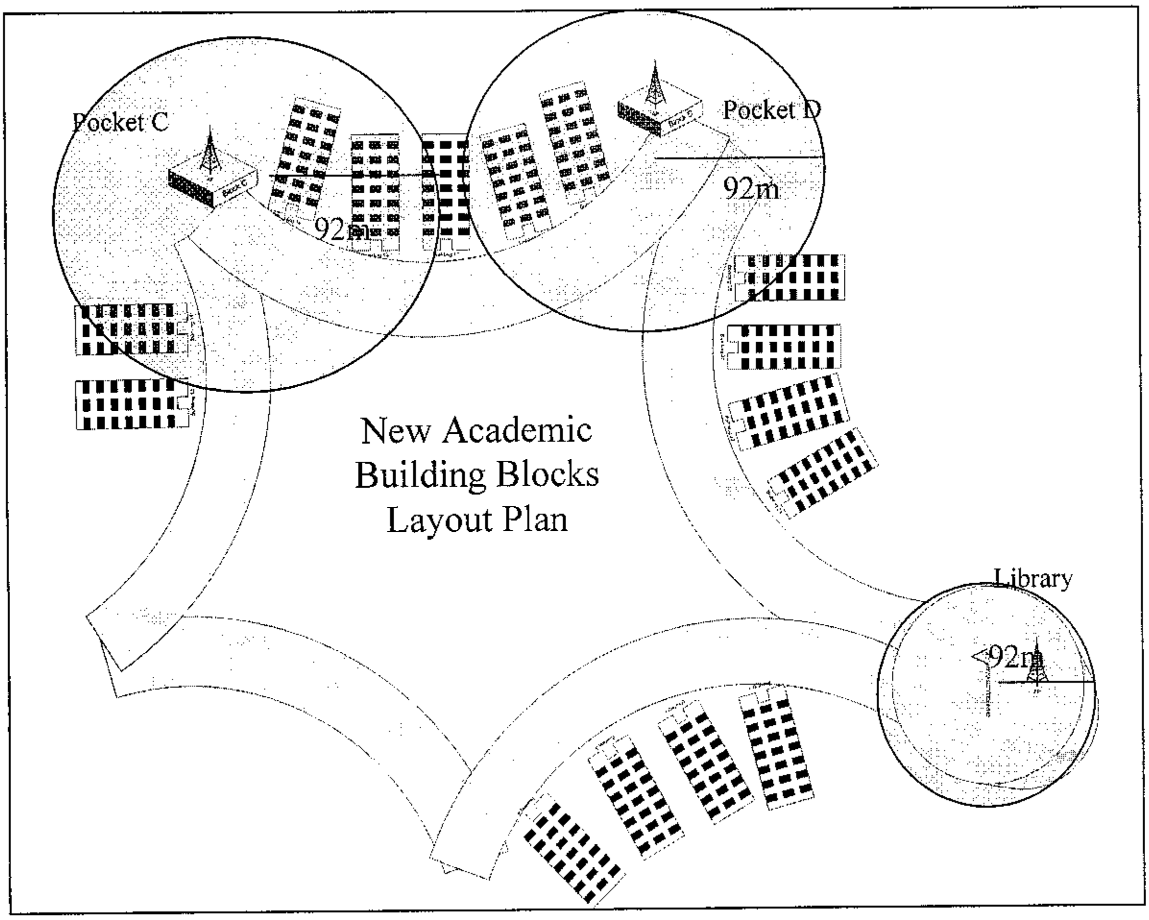
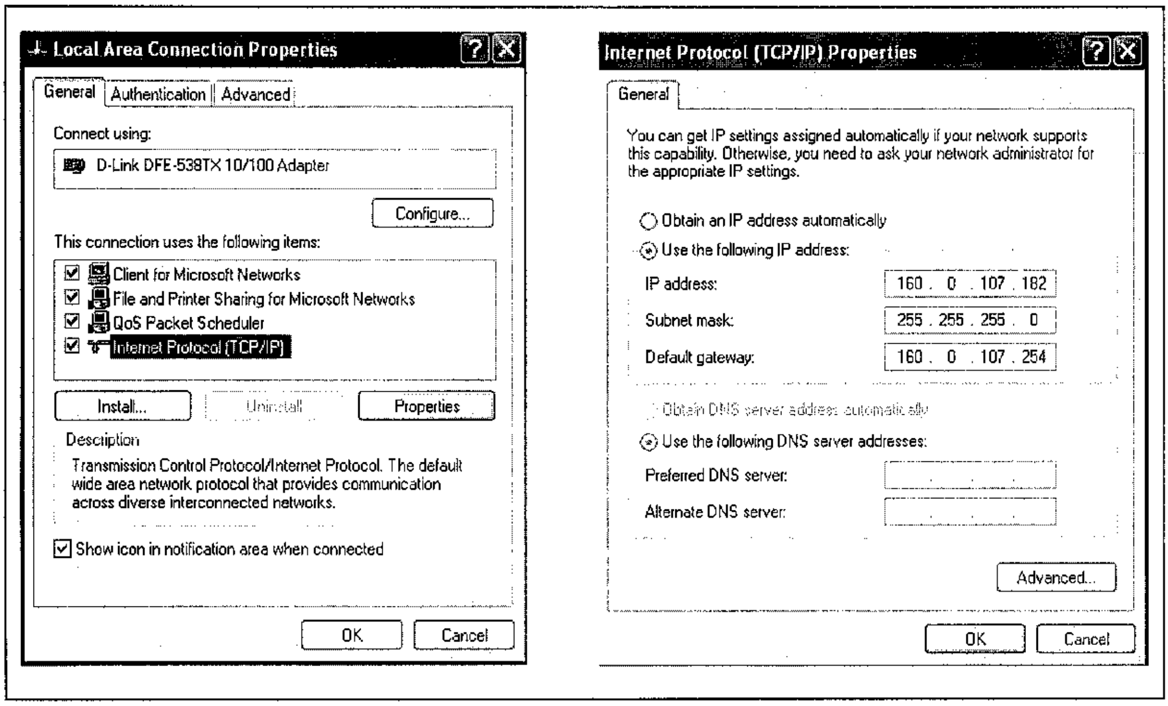


Figure 20: Academic Block Coverage Area

For the academic block areas (Figure 20), manual configuration of IP is used. Thus, students are required to set the IP of their computer manually to get access to the network (Figure 21).



Connect using:

D-Link DFE-538TX 10/100 Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 160 . 0 . 107 . 182
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 160 . 0 . 107 . 254

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Figure 21: Configuring IP manually

4.3.4 Security Issues

Security for 802.11 networks can be simplified into two main components: encryption and authentication. The IEEE has specified that wired equivalent privacy (WEP) be the means to encrypt 802.11 data frames. WEP uses the RC4 encryption algorithm, a symmetric stream cipher for encryption. A stream operates the encrypt or decrypt function on a unit of plaintext (in this case, the 802.11b frame). With symmetric encryption, the key must be shared by both the encrypting and decrypting endpoints. A mechanism is used to ensure that the same plaintext will not generate the same ciphertext. The IEEE stipulated the use of an initialization vector to be concatenated with the symmetric key before generating the stream ciphertext. Thus, with the use of frame encryption, security of a WLAN can be increased.

Meanwhile, for authentication method, the IEEE specified two authentication algorithms for 802.11-based networks. They are open authentication and shared-key authentication. Open authentication is a null authentication algorithm where any station requesting authentication is granted access. Meanwhile, the second authentication method, shared-key authentication, requires that both the requesting and granting stations have matching

WEP keys. This means, when a requesting station send an authentication request to the granting station, the granting station will send a plaintext challenge frame to the requesting station. The requesting station WEP will have to encrypt the challenge frame and sends it back to the granting station. The granting station attempts to decrypt the frame. If the resulting plaintext matches what the granting station originally sent, then the requesting station has a valid key and is granted access.

With these two standard methods; encryption and authentication, the security of the users using the WLAN can be assured. Meanwhile, for physical security of the access point, it is suggested that the access point is located using 'high-end' method. This means, the access point is located at a high place, where it is harder for people to do something to it. It is also recommended that the access point is placed in a box, with holes for the antenna, so that it can be physically secured.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

The WLAN has its pros and cons. As users gained the advantages of WLAN such as mobility, security and reduce of cost, the users have to settle with a slower network speed. The WLAN is also vulnerable to interference, especially when infrared is used. Thus, radiowave might be a better solution when deploying WLAN in the campus. This means, Wi-Fi is much better to be used in the campus area. Wi-Fi which is using the 802.11 protocols provides 802.11a, 802.11b and 802.11g protocols that have its own advantages and disadvantages. The most used protocol currently is 802.11b protocol. One of the local universities, which is Multimedia University, is using this protocol for their Wireless LAN. Wireless LAN is certainly much slower than wired LAN, but it provides mobility and portability to the users, and allows network access without the limitation of wires. It is also cheaper compared to the wired LAN. The deployment of WLAN in other campuses in Malaysia is a great example of how the WLAN can be benefited from it. WLAN provide an access to the network to the campus users when they are away from the wired LAN. Thus, deployment of Wireless LAN could benefit the students and the other staffs when they are in the campus area.

For the future, it is recommended that performance and usability testing to be done on the suggested design. Also, the deployment of Wireless LAN in all area around the campus would be a good approach for the students to experience the wireless technology. The implementation of the Wireless LAN will provide a good environment for the students all around the campus, and let the students get connected to the network, anytime, around the campus.

REFERENCES

1. Louis, Stone-Collonge. 26 October 1998, *A wireless LAN unfettered by pigeons* <http://www.lantimes.com/98/98oct/810b014a.html>

1. Fisher , John and Wang , Rosemary <http://www.pdamd.com>

3. Welcher , Peter J. 8/6/2002, *Wireless LAN* <http://www.netcraftsmen.net>

4. Rob Schenk, Andrew Garcia, and Russ Iwanchuk, 2001 <http://www.extremetech.com>

5. Lough,Daniel L, Blankenship,T. Keith, Krizman,Kevin J. 1997, *A Short Tutorial on Wireless LANs and IEEE 802.11* <http://www.computer.org/students/looking/summer97/ieee802.htm>

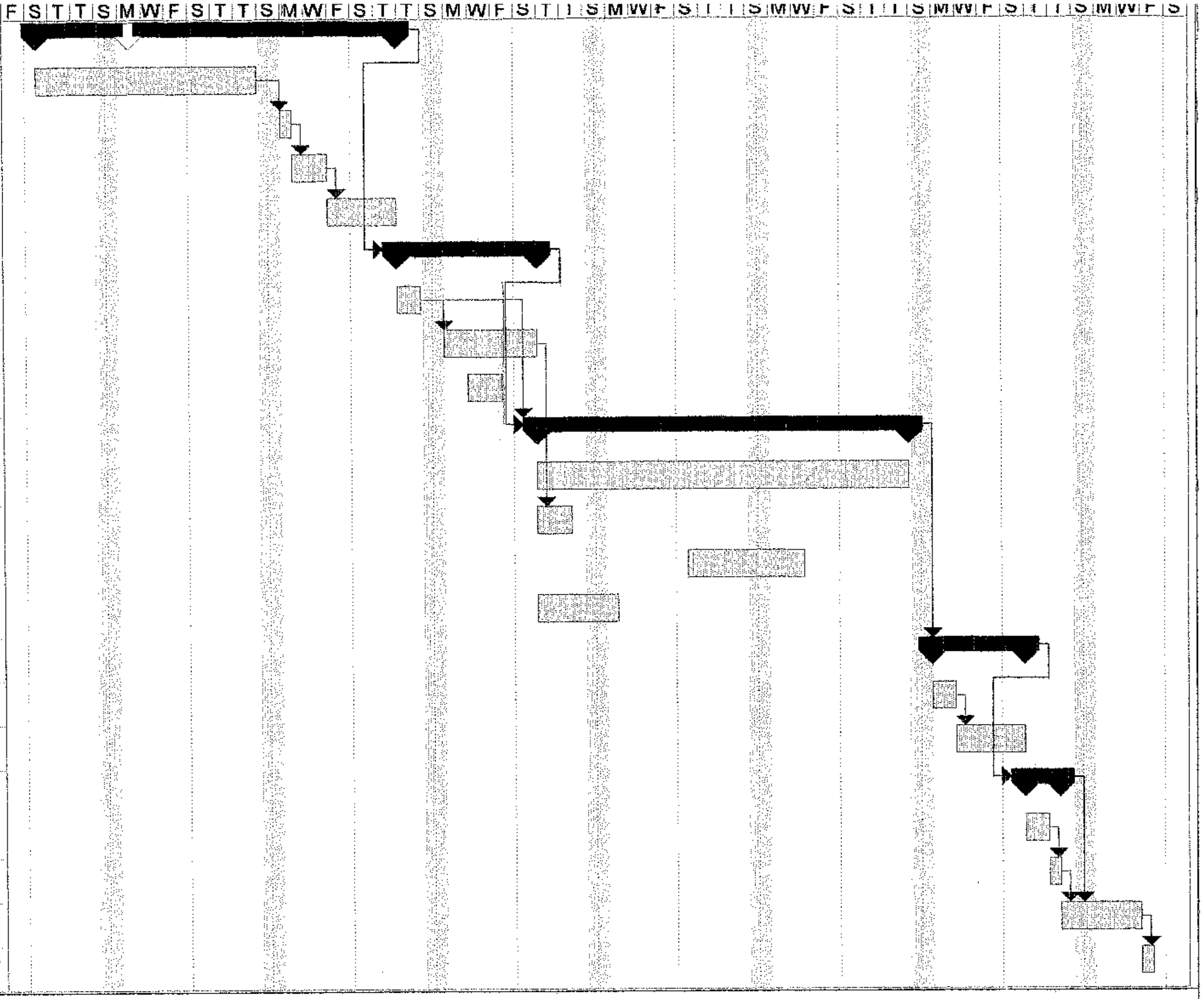
6. http://www.cisco.com/application/pdf/en/us/guest/netsol/ns178/c649/ccmigration_09186a00800d67eb.pdf

APPENDICES

APPENDIX 1:

PROJECT SCHEDULE

1	**Preliminary Study**	**Mon 7/19/04**
2	Project proposal & approval	Mon 7/19/04
3	Define problems and requirements	Mon 8/9/04
4	Project analysis and requirements	Tue 8/10/04
5	Methodology Formulation	Fri 8/13/04
6	**Project Requirements**	**Thu 8/19/04**
7	Construct questionnaires	Thu 8/19/04
8	Distribute questionnaires	Mon 8/23/04
9	Identify tools used	Wed 8/25/04
10	**Project Research & Analysis**	**Tue 8/31/04**
11	Internet research	Tue 8/31/04
12	Analyze questionnaires result	Tue 8/31/04
13	Analyze current wired LAN design	Mon 9/13/04
14	Interview	Tue 8/31/04
15	**Network Design & Development**	**Mon 10/4/04**
16	Review Design Sample	Mon 10/4/04
17	Construct WLAN Design	Wed 10/6/04
18	**Evaluation**	**Tue 10/12/04**
19	Review constructed WLAN Design	Tue 10/12/04
20	Improve WLAN design	Thu 10/14/04
21	Completed design and report	Fri 10/15/04
22	Final presentation	Fri 10/22/04



Project: Wireless LAN in UTP Campus

Task	▨	Milestone	◆	External Tasks	▨
Split	⋯⋯	Summary	▬	External Milestone	◆
Progress	▬	Project Summary	▨	Deadline	⇩

APPENDIX 2:

QUESTIONNAIRES FOR STUDENTS

Year ____

Program ____________________

1. Do you have a computer/laptop?

i-Yes ii-No

2. How do you rate the current LAN?

i- very good ii- good iii- average iv- need improvement v- bad

3. What do you think of deployment of Wireless LAN around the campus?

i- Very necessary ii- necessary iii- no difference iv- unnecessary v. waste money

4. Where are the suitable locations for the WLAN coverage? (choose as many as you like)

i- Cafeteria

ii.- Outside academic buildings

iii.- Library

iv - Lecture halls

v.- Rooms

vi.- Common room in every block

Others: (Please Specify); ____________________________

5. If there were to be WLAN in the campus area, how often will you use it?

i. Very often ii. Often iii. Sometimes iv. Seldom v. Never

6. How much are you willing to spend for WLAN devices?

i. Below RM100

ii. RM 101 – RM 200

iii.RM 201 – RM 300

iv .RM 301 – RM 400

v. Don't mind, as long as can access the facility

7. What are the applications that WLAN is used for?

i. Emails

ii. Access E-Learning

iii. Research

iv. Others (please specify) ____________________________

APPENDIX 3:

QUESTIONNAIRES FOR THE INTERVIEW

1. Can you please explain about UTP current setup?
2. Where are the locations of the switches in UTP?
3. What is your opinion if WLAN were to be deployed in UTP campus area?
4. From your expertise, where do you think are the suitable locations to setup WLAN? Why?
5. Which is more costly, setting up WLAN using the current network, or setting up new network?
6. What about setting up WLAN in the library? Are there any constraints?
7. When setting up WLAN in the village café, which switch is suitable to be used? The passport or the switch in on of the blocks?
8. What are the differences of using the switch in the students' block, and passport at the data centre at the village?
9. How many users can be supported if the switch in the block is used?
10. What about number of users if the passport in the village centre is used?
11. What about the place to put the AP?
12. Can you explain about the setting of IP if switch in the residential block is used? What are the differences if passport in Data Centre is used?