WLAN PLANNING AND CONCEPTUAL DESIGN IN UNIVERSITI TEKNOLOGI PETRONAS

By

Maniza binti Mansor

Dissertation submitted in partial fulfillment of

the requirement for the

Bachelor of Technology (Hons)

(Information System)

DECEMBER 2004

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzhuan
Tel: 05 3721100 Fax: 05 3721286

CERTIFICATION OF APPROVAL

WLAN Conceptual Planning and Design in Universiti Teknologi PETRONAS

by

Maniza bt Mansor

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

Approved by,

_____
(Mrs. Michelle Beh Hooi Cheng)

UNIVERSITI TEKNOLOGI PETRONAS

TRONOH, PERAK

December 2004

CERTIFICATION OF ORIGINALITY

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

MANIZA MANSOR

TABLE OF CONTENT

LIST OF FIGURES

LIST OF APPENDICES

ABSTRACT

Wireless Local Area Network (WLAN) is one of the new networking environments where it supports the mobility of the network user without being encumbered by the cable existence. Since the current Local Area Network (LAN) in Universiti Teknologi PETRONAS (UTP) is fairly growth and the performance reliability is good shifting the current setup to WLAN is locally accepted. This will benefit all the UTP users including students, respective lecturers, and beneficial for administration line of staff. The current planning and setup will cover certain stages in order to build a high reliability and best performance of the WLAN environment. Data transmission and signal strength for the area is fairly surveyed in order to result the best performance and ability to transmit data in bit per second required.

Research and questionnaire have also been done throughout the UTP students, IT Media Services Executives, respective IT Consultants from KLCCB Project Berhad in order to determine the best design concept to be applied in UTP campus and to determine the best place for WLAN to be implemented. Usage models are also needed to be determined in order to support the activity that will be in the WLAN environment. The conceptual design of WLAN environment will cater the area of the student residential including the Student Center, cafeteria, and residential buildings for Village 3,4 and 5. With help of this design it will be easier to determine the location of all the devices such as the wireless access point (AP) and security access point (SAP) as to roam the signal coverage and to secure the signal for data transmission. The technology use in data transmission is also being covered in this research paper, which includes the Spread Spectrum LAN. As to meet the problem statement requirement to ensure the system meets the budgeted cost, the author came out with the budgeting plan for all the devices allocated for the WLAN setup. The WLAN planning and setup in UTP research will help the UTP management in getting the grasp idea how to setup WLAN environment in UTP campus and to compliance with the current LAN setup and to secure the cost and budgeting for all devices related.

ACKNOWLEDGEMENT

The author would like to take this opportunity to express his deepest gratitude and thanks to Universiti Teknologi PETRONAS. The university has provided a basic module for the students to establish their own project. This Dissertation Report might not be completed without cooperation and support from the following individual or group.

1. Mrs. Michelle Beh (Final Year Project Supervisor)
2. Mr. Johari Surani (KLCCB Projeck Berhad IT Consultant)
3. Mr. Mohd Nizam Shamsuddin (Teliti Computers Sdn Bhd Network Engineer)
4. Mr. Nazri Nasir (Universiti Teknologi PETRONAS IT & Media Serives IT Executives)
5. Mr. Ruslan Razali (UTP Data Communication Lab Senior Technician)
6. Final Year Project Committee
7. Resource Center Of Universiti Teknologi PETRONAS
8. Universiti Teknologi PETRONAS lectures, technicians, staffs and students

CHAPTER 1
INTRODUCTION

1. 1 BACKGROUND OF STUDY

The mobility of the LAN user enforces the technology to evolve for wireless. The aim of this project is to produce a complete proposal of network planning and design for Wireless Local Network (WLAN) in Universiti Teknologi PETRONAS .The objective of this project is only to cater the planning and design of the Wireless LAN that will cover certain area in deploying it. It also caters the total shifting from the Local Area Network (LAN) to Wireless Local Area Network (WLAN). This project will overcome certain problem regarding the Wireless Local Area Network (WLAN) deployment in term of performance, reliability, connectivity, interoperability, expandability, manageability, centralization of services for ease support and maintenance and also protection of investment for future upgrades. The scope of the of this project is divided into 5 part which are overview of the WLAN, functions and network components, WLAN environment and topology which include site surveying, WLAN security, and conceptual design. Methodology applied is called Hypothetic-Deductive.

The network for Universiti Teknologi PETRONAS was designed as three (3) tiers network with a comprehensive triangle backbone to support a very effective link redundancy. All tiers were strengthened by Passport 8600, supporting all the edge switches from the distribution sources. This comprehensive triangle backbone was taking place on supporting the entire major backbone link and this designed triangle will avoid any downtime from occurred.

Three passports supporting this major backbone are located at three different strategic places, which are Data Center, Pocket C and Village Center 3. All this three places are definitely strategic in supporting particular cases in this wide campus area of massive activities by students and lecturers.

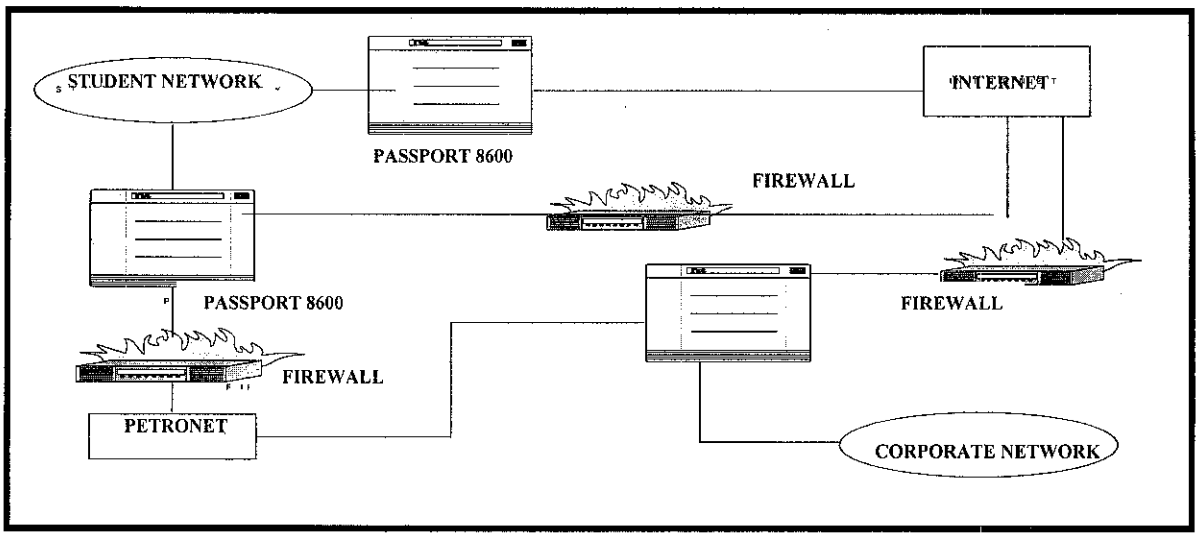


Figure 1: Network Type and Network Tiers (Passport 8600)

As shown in Figure 1, There are 2 types of network in UTP which is the Corporate Network and Student Network. Corporate network has a direct link to the PETRONAS website and server called PETRONET. This Corporate Network only grants it access to the UTP staff in every department (IT Media and Service, Human resource, Finance Department etc). Student will not have any access towards this network. It has been block with certain firewalls located at the Data Center. For all UTP students, they will only be granted an access to Student Network. This network can access to the Internet and local intranet (example e-learning, MPP forum etc). As to follow the PETRONAS policy, every login session should pass the Novell Border Manager. This Novell Manager will limit the bandwidth of every packet of data transaction in certain sessions. Every student and staff has their own ID before log-in into the system. Different ID will be remarked as different user, in order to get through the Corporate or Student network. The Novell Border Manager Server is also allocated at the Data Center.

All the network setup in UTP will be hosted from the Data Center (located at Main Chancellor Building basement). From data center the connection will be routed back to the New Academic Building including Pocket C, D and old administration building, and it also covers the connection to all student residential (Village 3, 4 and 5).

To adapting the WLAN in the student residential, design should be made based on the current LAN in UTP. Students should only have an access to Student Network and bypass the Novell Border Manager as following the PETRONAS policy.

In this research paper, the shifting of the WLAN will be done towards the most suitable place based on the performance of the signal transmission, signal strength and less interference. Usage models and capacity of user in certain location also will be taken into account in order to implement well applicable WLAN area. Considering to the standard of the devices used during the installation is compulsory, in order to make it compatible with the current LAN setup in UTP. As a result, the budgeting also will be secured and future upgrading can be easily implemented. Certain technique and discussion with the expert is done by the author in order to get data regarding the usage models and capacity of user in certain area. This will be discussed more later in Chapter 6. Three potential places which are suitable of shifting to WLAN area as follows :

- Student Residential Facilities (cafeteria, student lounge, KOPETRO, and laundry room)
- Student hostels (Village 3 , 4, 5)
- New Academic Building (recreation area).

Site survey will be done to all of these areas to determine the best place to allocate to WLAN services. The other important thing need to be considered in the WLAN setup is the technology used to transmit data in the wireless environment. There are certain types of technology used such as the Spread Spectrum LAN, Low Power Narrowband, HiperLAN and Infrared LAN. However, in this research the author will be more focusing on the Spread Spectrum technologies which comply with 2 methods of data transmission.

- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)

WLAN security is also important during the implementation. With regard of the security threats that usually manifest the WLAN environment are:

- Eavesdropping
- Attacks from within the network neighborhood
- Unauthorized access

These security issues not only effect the WLAN but also the current LAN in UTP. To automate the well secured WLAN, the author decided to adhere with the current LAN setup which protects the WLAN environment using certain gateway and firewall and authorization given towards every user into the network.

Hardware selection is also important in establishing the WLAN. The current LAN setup in UTP is using all the devices provided by Nortel Networks. All of the devices is adherence with the IEEE 802.11 standard with the Plug and Play wireless Ethernet products. Nortel Network WLAN 2221 series offer an enhanced user experience through true mobility, total security and integrated management, with the intelligence and performance for mass deployment of multi-service wireless network. The WLAN 2221 access point offers 802.11b radio technologies, which offer transmitting signal throughput of 11 Mbps.

To support all the findings the author will run 4 demonstrations regarding the step by step taken in order to implement the WLAN environment in UTP. However, all the devices used for the demonstration purpose is from the CISCO Network. It will guide user on how to run a site survey, to check the signal strength and noise distortion toward certain area, to setting up an infrastructure WLAN connection and how to configure the access points, antenna and DHCP server for the IP configuration. The demo will also cover how to setup a secure wireless LAN environment.

All the results and findings will help the author in designing the conceptual plan of the WLAN in UTP and the coverage area of the best location to be shifted to WLAN environment. The conceptual plan will include the coverage area of the signals and bit per second transmitted, the location of the access point, antenna and the routing of the network from the respecting WLAN server to the UTP main core network node (Pocket C, Village 3 and Data Center). The conceptual design will include the current setup of UTP Local Area Network, and type network that will be allowed bypassing certain server. In UTP there are 2 type of network including the Student Network and Corporate Network. Gateways will only allow the person logging in as Corporate Network to access the PETRONAS Internet (PETRONET) from the main headquarters (PETRONAS Twin Tower) and not for the person who log in as Student Network. All of these activities will also be protected with certain firewalls as for security concerns.

For this project the author's target is to come out with the best planning of WLAN in UTP campus with the lowest budget but securing the system performance and capability of WLAN environment in supporting user activities.

1.2 PROBLEM STATEMENT

1.2.1 Problem Identification

1.2.1.1 Performance

i. To increase throughput and shorten respond time for accessing the system.
ii. To increase the efficiency and the effectiveness of the IT system.
iii. To provide a more robust network infrastructure system, structured signal and cable plant, network component such as intelligent network component such as intelligent hubs/switches and high end servers

1.2.1.2 Reliability & Stability

i. To provide a more secure environment at the hardware and software level.
ii. To reduce down time for accessing any of the IT services.
iii. To have redundancy and alternatives physical and logical paths.
iv. To provide a robust network infrastructure thorough a high reliability network component.
v. To provide a network infrastructure which is tolerant to changing traffic condition.

1.2.1.3 Connectivity

i. To accommodate Open System/Distributed Computing Environment.
ii. To support multi protocols.
iii. To ensure the integrity of the voice, data and video system.

1.2.1.4 Flexibility & Interoperability

i. To integrate the IT system into the enterprise network and integrate Campus Area Network.
ii. To be able to mix and match between different vendors products.
iii. Standard based on the greatest interoperability between equipment in between vendors.

1.2.1.5 Expandability

i. To accommodate the network future growth such as the bandwidth of the data, traffic integration etc. so that the new technology can be easily incorporated when it become feasible in Universiti Teknologi PETRONAS (UTP).
ii. To expand without requiring major network redesign or causing the degradation of network performance

1.2.1.6 Centralization of services for ease support and maintenance.

i. To centralize all the file server and common system at Data Center. All servers shall be commonly accessed by the user in UTP campus.
ii. To centralized the WLAN to remaining Data Center and allow centralized management of the system and supports.

1.2.1.7 Protection of Investment

i. Use of the existing hardware and software as much as possible.
ii. Securing the cost constraint of shifting to WLAN environment.
iii. Incorporating the new technology and component must be upgradeable or being used in other areas of the business.

1.2.2 Significant of the project

Able to come out with the plan of the WLAN environment shifting in UTP campus. Also be able to stimulate the result and findings into certain demonstration. To come out with a planning and the allocation of the hardware such as access point and the antenna. To determine the best coverage area and the suitable usage model before setting up the WLAN environment.

1.3 OBJECTIVE AND SCOPE OF STUDY

1.3.1 Site survey.

i. Usage models.
ii. Capacity of user
iii. Coverage area and signal strength
iv. Type of signal interference

1.3.2 Suitable transmission medium technology concentrating on the Spread Spectrum LAN which can be categorized under 2 methods:

i. FHSS (Frequency Hopping Spread Spectrum)
ii. DSSS (Direct Sequence Spread Spectrum)

and comparison for both medium which suitable for be adapted in the current setup in UTP campus.

1.3.3 Be able to cater the security issues regarding the transmission medium security issues that include eavesdropping, unauthorized access and the other attack from the network neighborhoods.

1.3.4 To come out with the conceptual design of the signal coverage area of selected places, the access point allocation, and the antenna location to cater the best bit per second transferred in every transmission.

1.3.5 Hardware decision for installation.

i. Surveyed toward hardware suitability and compatibility in UTP.
ii. Most recently used hardware used for installation
iii. Access point standard comparison (802.11a, 802.11b,802.11g)
vi. Hardware allocations taking consideration into constraint (cost, recent operation compatibility, operation performance)
vii. Come out with the price quotation and costing towards all the devices installed during the setup.

1.3.6 Be able to demonstrate the result and findings into 2 stimulations.

i. Site survey

ii. Access point

CHAPTER 2
LITERATURE REVIEW

Wireless Local Area Network (WLAN) is becoming increasingly popular nowadays. It is compatible with the wireless network devices such as PDA's, cell phones, notebook computers or handheld game that can be connected to the Internet or private intranet. Without the existence of cables, user can send email and downloaded files. The freedom to move about without being tethered to the network by wires is one of the WLAN advantages.

There are certain types of network configuration based on geography, one of them is Local Area Network (LAN).The Local Area Network is type a of network that specified by the IEEE Standard for local networking which capable to cover a few blocks and few miles. This LAN network has usually been applied in university campuses where it cover all the academic and administrative purposes. As nowadays people adhered toward mobile networking the enhancement of LAN is shifted to Wireless LAN (WLAN). There are many advantages to a WLAN, including mobility, easier and less expensive installation, easier network modification, increased network reliability and speedier disaster recovery.

Wireless is becoming increasingly popular. They are common place on university campuses and inside corporations, and they have started to appear in public areas [1]. Edward C. Prem (2000) says that the mobile users require that they are connected to the network regardless of where they are because they want simultaneous access to the network [2]. WLAN have the ability to adjust the conditions and also to configure them to make it the best used with available bandwidth.
According to the Institute of Electric & Electronic Engineers (IEEE), Wireless Local Area Network (WLAN) is a data communication system usually owned by a single organization that allows similar or dissimilar digital devices to talk to each other over a common transmission medium [3].

A Wireless Local Area Network is distinguish from other types of data networks in that communication moved to mobile and it confined to a moderate geographic area such as a single office, a warehouse, or a campus, and can on depend on a physical communication channel of moderate-to high data rate which has consistently low error rate [4].

The concept of WLAN may be used to connect data devices such as computers, terminals, mass storage devices, and printers/ plotters. Through the network these devices can interchange data such as file and electronic mail. However, all the interest is generated by the WLAN promise as a means of interconnecting various computers into a systems that is more useful than their individuals parts. The goal of WLAN is to provide a large number of devices with inexpensive yet high speed local communications [4].

WLAN network planning and design are phases that involved development and implementation of IT infrastructure. The development or implementation of such infrastructure involves many stages. The most important things to be considered are the current setup of the network topology in the area. According to Ata Elahi, Ph.D author of the Network communication Technologies Delmar Thomson Learning, network topologies are the way computer connected together. The technology used in WLAN will help the transmission of the data throughout the WLAN environment. Some of the technologies are the Spread Spectrum LAN, Low Power Narrowband, HiperLAN and Infrared LAN.

Universiti Teknologi PETRONAS (UTP) basically has a current setup of LAN connected through the hierarchical of star topology network. Two types of networks in UTP which is the Corporate Network and Student Network. Corporate Network has a direct link to the PETRONAS web and server called PETRONET. This Corporate Network only grants its access to the UTP staff in every department (IT Media and Service, Human Resource, Finance Department etc). Student will not have any access towards this network. It has been blocked with certain firewalls located at the Data

Center. For all UTP students, they will only be granted an access to Student Network. This network can access to the Internet (World Wide Web) and local intranet such as e-learning, MPP forum. It will be easy to shift to WLAN using the star topology and it is very easy to set up and expand the network. It is reduce cost and enhance the performance of the WLAN itself.

The types of technologies used to implement WLAN are very diverse. Users are compelled to make choices that will be based into certain criteria:

1. Network topology and architecture
2. Access control
3. Transmission medium
4. Transmission technique
5. Adherence to standard

Adherence to standard used for the hardware is also important during planning. As WLAN network topology concerns, certain standard compelled to it are 802.11, 802.11b, 802.11a, 802.11g. Certain standard applied towards the specification of the Wireless LAN and different peripherals vendor might be differ. CISCO Security is one of the vendors that involved in supplying all the devices, installation and providing the technical specification. The specified standard for the WLAN is 802.11a or 802.11b depending on the approaches that have been applied in the Physical layer under the OSI model. It deals with different frequencies and encoding methods.

Security issues also need to be included into this planning and setup. It is a mistake to assume that the vulnerability level of a wired LAN is lesser than a Wireless LAN. According to the article written by *Melanie McMullen* (1998), wireless communication (specifically spread spectrum) was first introduced and developed for military purposes and one of its early patents was for torpedoes guiding system. This was a system that requires an extreme security transmission service.

Moreover, a result from a survey done by *Venture Development Group* indicates that almost 30% of usages of wireless LAN are from financial and government institutions. All of these institutions make use of data transmission that requires the highest level of security.

Site survey is also important in planning the IT infrastructure. It is important to place the Access node at the location with less interference and noise distortion that will distract the signal while transmitting the radio frequency (RF) signal. This RF signal transmits all packets and decoded to the transmitter and send it back to the receiver via the wireless network interface card (NIC). This also involved the process of decoding back the packets into understandable signal to the workstation. Site surveyed will be done in checking the signal strength in selected area which covers the area of Student Residential Facilities (cafeteria, student lounge, coop, and laundry room), Student hostels and New Academic Building (recreation area). The surveyed includes the signal strength percentage coverage area, the link quality, link speed and the frequency of the area surveyed.

In addition, usage models are also important in the planning. This will helps in determining the minimum bandwidth for each simultaneous user. The types of applications that users will run while connected to the WLAN. The expected usage will be different at different sites. In determining the simultaneous user, questionnaire is done to determine the peek hours of the service used and maximum capacity of user can be allocated into certain area.

The successful of the WLAN setup is determined if all of the elements required is implemented. The shifting network topology to WLAN will allow all users in the UTP campus to interact wirelessly without encumbered by cable existence.

CHAPTER 3
METHODOLOGY

3.1 Hypothetico-Deductive method

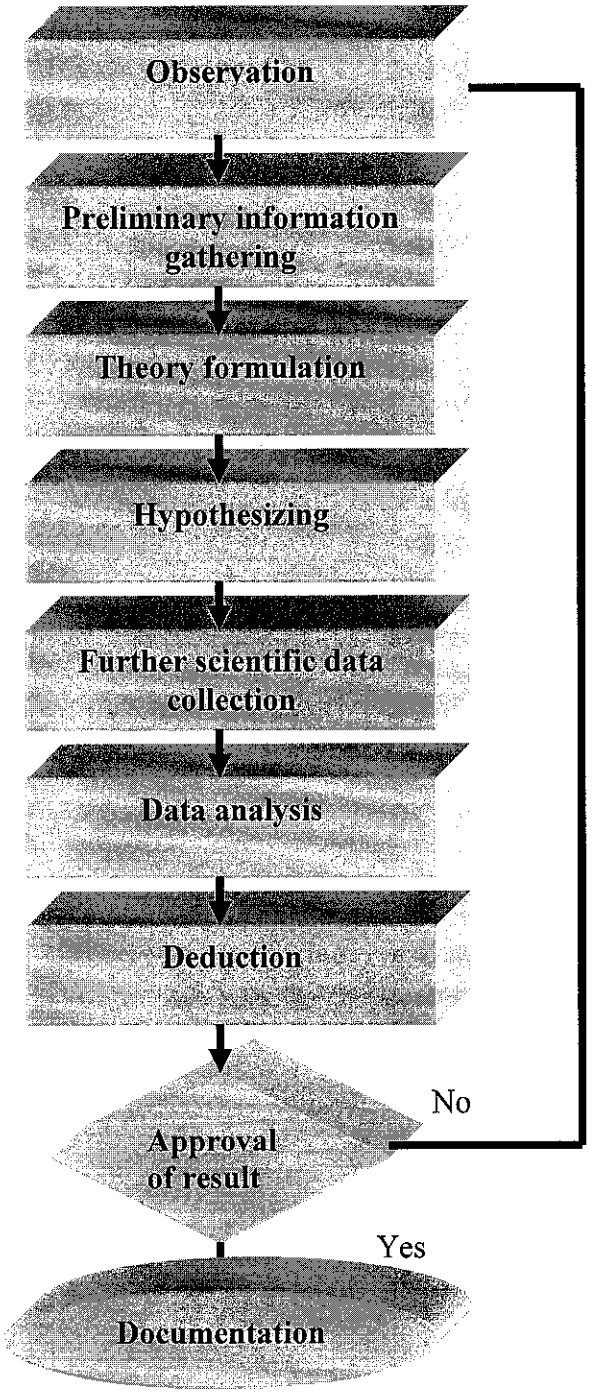


Figure 2 : Flow chart of Hypothetico-Deductive method

3.1 Hypothetico-Deductive method

It comprises different stages that will be guiding the author towards the research. The step will also cover the data gathering, literature reviews, site surveying, and final result and report. The stages include:

- Observation: In this stage the author will be describing the major area of research, determining the scope of studies, problem statements and the proposed solutions towards the problem.

- Preliminary information gathering: Literature reviews and the journals have been reviewed for further supporting of the research. Related journals will be gathered before come out with the theory.

- Theory formulation: This is where the theory is adapted toward the research progress. The idea from the literature review will be quoted and as reference before the author do her own hypothesizing. Theory formulation also include the site surveyed done in the area.

- Hypothesizing: It will supported all the theory formulated and as a guidance towards the further scientific data collection. It will include the questionnaire and interview session as to support the hypothesis made.

- Further scientific data collection: As to further support the hypothesis, data collection is done. In this step, interviewing the expert majoring in the networking fields is done. The result from the interview will be adapted to hypothesis made by the author with the current and real life WLAN environment.

- Data analysis: Suitability and compatibility of the data will be further analyzed by supporting ideas from the expert, and if there is certain malfunction occur during the hands-on of the peripherals and site surveyed. This data will be considered back and changes will be made under the next step. Alternatives of the changes are listed and test is being done towards the alternatives in order to suit best with the planning.

- Deduction: The best alternatives will be taken and data deduction will be done until the best result achieved. The finalize data and theory will be compiled into final dissertation, and towards the planning of WLAN in UTP.

3.2 Tool required

Tool required on this research is base on the stages of the research progress.

- Site survey and signal strength determination towards selected area
    i. CISCO Aironet System Network Software – design for the site surveying and signal transmission setting for WLAN environment.
    ii. Laptop equipped with wireless interface card (NIC)
    iii. UTP current LAN connectivity
    iv. WLAN – Mobile Adapter 2201 (with its unique 802.11a/11b roaming capabilities
    v. WLAN – Access Point 2220 and the WLAN – Security Switch 2250

- Hardware involved during installation caters :
    i. Passport 8600
    ii. Business Policy Switch 2000
    iii. Cascade Module
    iv. WLAN Access Point 2221
    v. GBIC MDA – Gigabit Interface Converter Media Dependant Adapters
    vi. WLAN Security Switch 2250

- WLAN Conceptual Design phase
    i. Microsoft Visio 2000
    ii. AutoCAD 2000

CHAPTER 4
RESULT AND DISCUSSION

4.1 Usage models

It is important to know the layout of number of user and the user density of user per unit area. The number of user will determine the bandwidth required. To get the result, questionnaire is segregated to students.

Result :

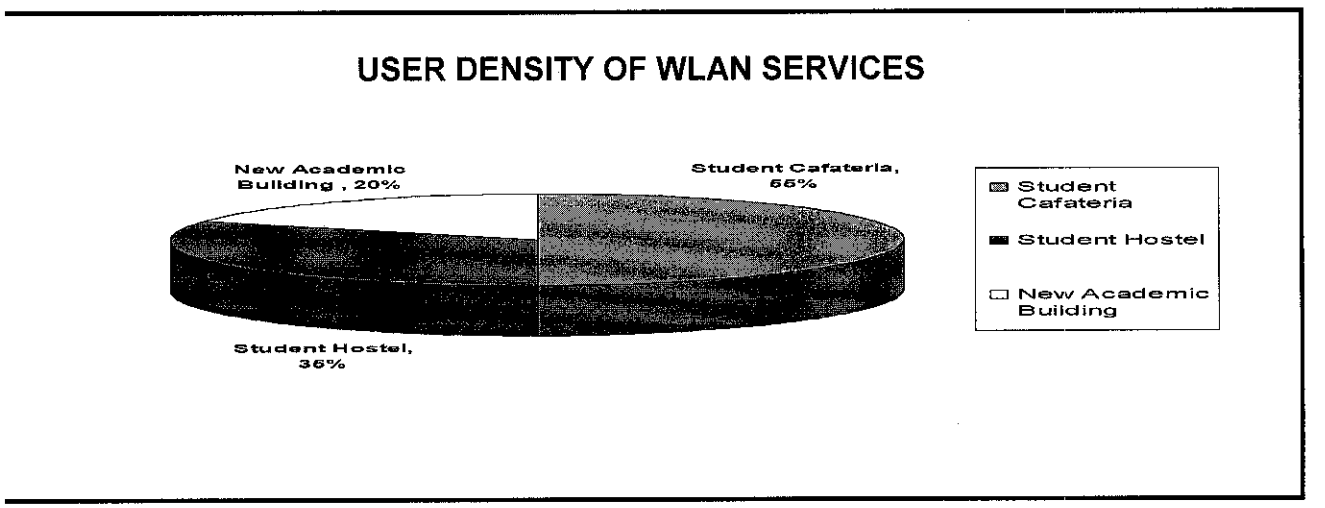


Figure 3 : Pie Chart Indicating the User Density of WLAN services

Discussion :

From the survey it shows that almost 55% percent of UTP student prefer WLAN in cafeteria since they do discussion and study group more in the cafeteria, and most of leisure time they spent at the cafeteria. 35% of the student prefer to go for wireless in their own room for their own conveniences, and 20 % of the student prefer to go wireless at the New Academic building (recreation area). Please refer Figure 4 for the result.

As the result from the area selected, the author will determine the peak hours that student will be coming to café and percentage of activity that will be done in the café based on certain criteria. The time of peak hours will be taken for every 2 hours, assuming that student will be in the café from 8 am until 12 midnight.

Results :

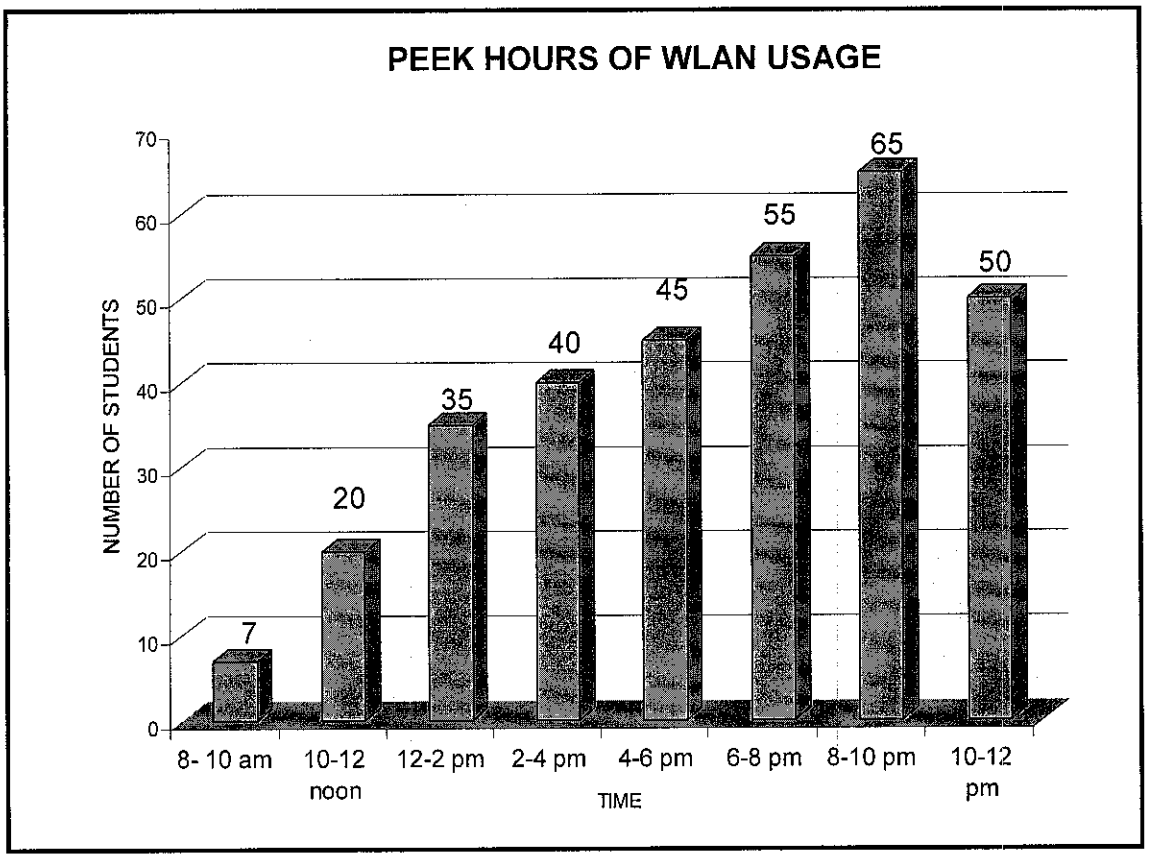


Figure 4 : Bar Chart Indicating the Peak Hours of WLAN Usage

Discussion :

As shown in Figure 4 ,the best place to implement the WLAN is the student cafeteria, Student Center which includes the student lounge, KOPETRO, laundry room and security room. Since the maximum user will be predicted is 65 - 80 people in the area at one time during the peak hour as shown in Figure 5 will be from 8pm to 12 midnight.

We can determine the maximum bandwidth that will be allocated to one user. In the typical sites it require at least *200Kbps and multiply with the simultaneous user*

Let assume that the number of simultaneous user is 20.

200 Kbps X 20 simultaneous users = 4000Kbps = 4.0 Mbps bandwidth needed.
For the access point (AP), one AP can provide coverage for the physical area of 20 - 25 users. During the planning number of AP needed will be 5 for each area. This will cover at least 100 users per session.

4.2 Technology

The transmission of the data is crucial in a wireless environment. There are certain categories of technologies used:

i. Spread Spectrum LAN
ii. Low Power Narrowband
iii. Infrared LAN
iv. Hiper LAN

However, as for this research purpose it will be only concentrated on the spectrum modulation technology for the Wireless LAN in UTP campus. Spread spectrum is a technique that spread a narrow signal over a broader portion of the radio frequency band. Spread spectrum is more resistant to outside interference. This is because any interference would only affect a small portion of the signals instead of the entire signal. Spread spectrum likewise resulted in less interference and fewer errors. It is also difficult to detect and intercept the signals during the transmission. Nonetheless, spread spectrum also reduces errors as the signal undergoes demodulation process at the receiver end. This is due to the fact that any interference would only affect a small portion of the spread signal. The usage of the spread spectrum signal does not require any special license from the authorities, provided that the devices used meet certain requirements such as frequency and coverage.
In the spread spectrum technology there are 2 common methods in data transmission:

i. FHSS (Frequency Hopping Spread Spectrum)
ii. DSSS (Direct Sequence Spread Spectrum)

FHSS transmits a short burst at one frequency then another short bursting at another frequency and so on until the entire signals have been sent. Frequency hopping can also reduce the impact of interference from other radio signals. An interfering signal will only affect the FHSS signal when both transmitted at the same frequency.

Because FHSS transmit a short burst over a wide range of frequencies; the extent of any interference will be very small and can easily be corrected by error checking. FHSS transmit a short burst on one frequency that is typically 1MHz. As a result it will create a minimal interference of other signals.

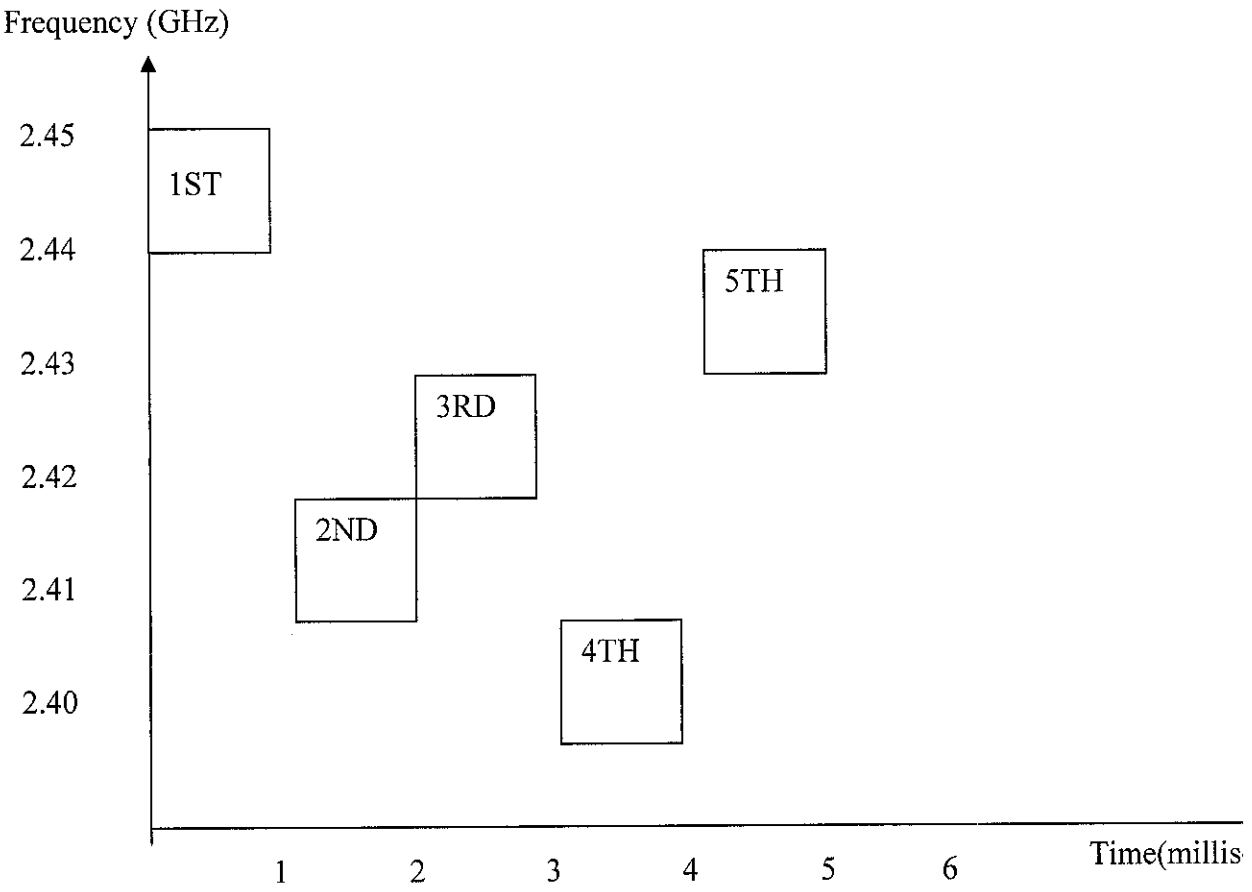


Figure 5 : FHSS Transmission.

DSSS generate redundant bit pattern to represent the bit needed to be transmitted. This pattern bit is known as chipping code. The recovery code is depending on how long the chipping code would make the recovery of the original data. In this process a large bandwidth is required for the network. DSSS require a high cost and utilize more power than FHSS. However DSSS WLAN has a potential for greater transmission speed rather than FHSS. DSSS transmit on a frequency that is 22MHz wide.

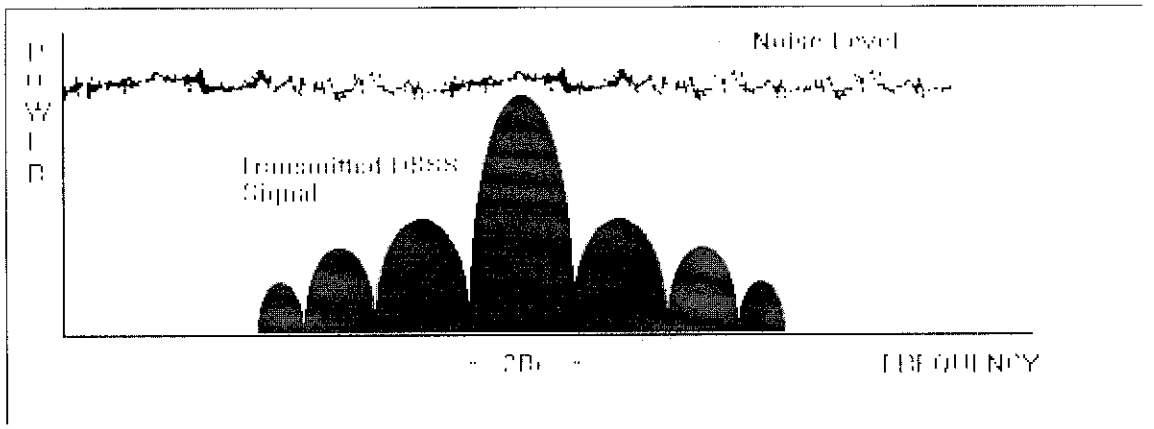


Figure 6 : DSSS Transmission

In this project, after considering the location and the area of the project, it is better to utilize the FHSS as the transmission medium. It is because FHSS involves in dividing a range of the radio spectrum into individual channels. Each of the channels is presenting one specific frequency. A data signal will then hop from frequency as a function of time according to a specifics pattern known as hopping code. In order to get the signal, the receiver must use the same hopping code while listening to the incoming data signal at the right time and on the correct frequency. It will also eliminate enormous errors.

4.3 Security

This element is crucial in implementing a WLAN to prevent certain hacking and intrusion risk. Nonetheless, the problems of security affect not only a WLAN but also the wired LAN environment. These are the common threats that usually occurred:

i. Eavesdropping
ii. Attacks from or within neighborhood
iii. Unauthorized access

To overcome this problem, below are the recommendations of the best practices can be applied in order to protect the transaction of the data in the WLAN environment.

4.3.1 FHSS Technology.

The reason why FHSS is implemented as a transmission medium because it can be used to provides security for the data signal. This transmission runs through the channels in a random sequence and allows the data to be on a channel for a fixed amount of time, and then transfer it to the next channel in the sequences. Without information concerning the "dwell time" (time spent on each channel) and the hopping pattern, it is impossible for the non-participating station to receive and encoded the data.

4.3.2 User Authentication or Local Station Password

This is important and it is a regular practice to the entire user to have their own login id as to authenticate them using the system, since it is more concerning the fact that WLAN support mobile users. Network OS such as Microsoft NT and Novell Netware provide built in security measurement such as user login and password. A strict passwords policy can ensure that a station can only be handled by the person assigned to. Ethically, password must be changed frequently.

4.3.3 Data Encryption

Data encryption can be installed using the third party software or hardware. This can be classified into the highest level of security that can be implemented in WLAN in UTP campus, since it deals with a large number of users with different data transactions. Basically all the data transmitted through the packets will be scrambled before it is sent over the LAN. The receiver from the other site must be able to encode or decrypt back the data using the decryption key and read the data.

4.3.4 Station Authentication System or ESS ID *(Extended Service Set Identifier)*

For the station to access the network or ESS, the access point would first check the station 32 characters ESS ID matches its own. Outside nodes, even having the same products, can participate in the network nor learn the hopping pattern, thus eliminate the possibility to eavesdrop. This ESS ID is programmed into the wireless adapters (SA-10 PRO, SA-40 PRO, SA-PCR and AP-10), under the control of an installer password and that changes can only be made on the adapters itself using HyperTerminal.

4.4 Hardware

4.4.1 Passport 8600

The Nortel Networks Passport 8600 series Ethernet Switch delivers a highly available, operationally simplistic, and intelligent network routing solution. In addition, hardware-based wire speed performance enables fast and efficient traffic classification, policy enforcement, and filtering. The Passport 8600 series Ethernet Switch delivers a robust, secure, and intelligent solution that provides a true competitive edge.

Passport 8600 will take place as the main back bone for UTP in delivering the data flow seamlessly all over the UTP wide area Network.
The Passport 8600 switch modules provide a full complement of core routing and switching capabilities in a Passport 8000 Series chassis. The Passport 8600 modules provide 10/100 megabit per second (Mb/s) auto-negotiating twisted pair Ethernet ports, 100 Mb/s fiber Ethernet ports, fiber and copper Gigabit Ethernet ports, packet over SONET, and ATM.

A Passport 8000 Series chassis with installed Passport 8600 modules constitutes a single switching entity with distributed management and full redundancy that delivers wire-speed routing and layer 2 switching.
The Passport 8600 modules include a switch fabric module and eight different input/output (I/O) modules. One switch fabric module is required for each Passport 8600 switch; for CPU system redundancy and double switch fabric capacity, you can install two switch fabric modules. You can install up to eight Passport 8600 I/O modules in a Passport 8010 chassis, and up to four I/O modules in a Passport 8006 chassis. The I/O modules support different types of Ethernet interfaces with different speeds, port counts, and media types, as well as packet over SONET and ATM.

4.4.1.1 Passport 8600 Key features and benefits

i. High availability - A Passport 8600 Ethernet Switch with Split-MLT improves reliability, redundancy and applications performance for the entire network.

ii. Operational simplicity - Passport 8600 technologies like multimedia filters reduce configuration time and speed up network deployment and fault finding.

iii. Superior intelligence - Integrated Layer 4 thru Layer 7 forwarding capabilities improve applications performance by allowing you to balance and direct requests to the most effective resource.

iv. Lower cost of ownership - Hot swappable components and full network utilization are designed to let you use what you pay for all the time. The lean architecture of the Passport 8600 decreases the number of network components, further reducing costs. Figure shown a model of single Passport 8600

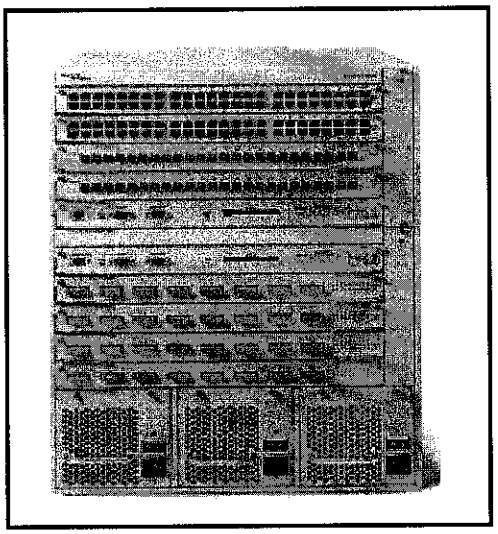


Figure 7 :Passport 8600 Accessories.

4.4.2 Business Policy Switch 2000

Business Policy Switch is a stackable Ethernet solution that delivers the industry's highest level of network availability, density, manageability and reliability. The Business Policy Switch is a stackable 10/100+1000 megabit-per-second (Mbps) Ethernet system.

BPS 2000 will task force as the edge switches, the inter media from the end users PC to the backbone. It is critical for edge switches to perform in a high availability and capacities manner to support the massive and robust users in using a high end superhighway like Passport 8600 backbone.

4.4.2.1 BPS2000 Key features and benefits

The Business Policy Switch delivers the high-performance IP infrastructure that can support the advanced IP telephony applications and requirements of the Business Communications Manager and the i2004 Ethernet Sets (IP Phones).

The Business Policy Switch acts as the stackable Ethernet edge or closet element in conjunction with the Passport routing switches in the network core, complements the Policy Enabled Networks line of products from Nortel Networks, and delivers end-to end QoS.

To further protect your network investment, flexible, high-speed LinkSafe up-link options (gigabit Ethernet/fast Ethernet/fiber) allow for connections to Passport routing switches, other high-speed switches, or the network center.

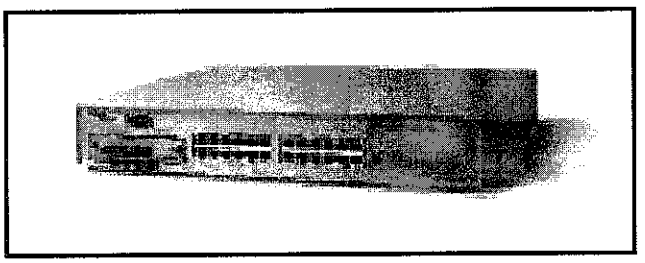


Figure 8: Model of single BPS2000

4.4.3 WLAN Access Point 2221

Nortel Network WLAN Access Point 2221 provides wireless solution for the new Village Network. The wireless access point will be placed at selected places to give the students the wireless features availability.

With its unique feature set and flexible architecture, Nortel Networks WLAN 2221 series offers an enhanced user experience through true mobility, total security and integrated management, with the intelligence and performance for mass deployment of multi-service wireless network. The WLAN 2221 access point offers 802.11b radio technologies, which offer transmitting signal throughput of 11 Mbps.

Anytime, anywhere access - that is the promise wireless brings; the ability to use the same applications you have access to from your desktop - no matter where you are. The nature of wireless - unrestricted by walls or doors - brings with it an inherent challenge: security. Add to this total cost of ownership, functionality, and manageability and you realize that up until now wireless LAN offerings have been unable to make the grade for the majority of enterprise customers.

Corporations want their wireless network to be an extension of their wired network. They seek standards-based solutions, which address security, QoS, interoperability and are capable of being managed by one system. The Nortel Networks WLAN 2200 Series makes it possible, by bringing the combination of True Mobility, Total Security, and Integrated Management into the enterprise.

4.4.3.1 WLAN Access Point 2221 Key features and benefits

True ability for users to maintain uninterrupted connectivity as they seamlessly roam across access points, different wireless technologies, subnets and buildings within the campus.

A layered approach to security, where modular or stand-alone solutions are available to suite customer requirements.

Simplified operations and reduces costs through easy configuration and intuitive network management. Below is the single model of WLAN 2221 Access Point

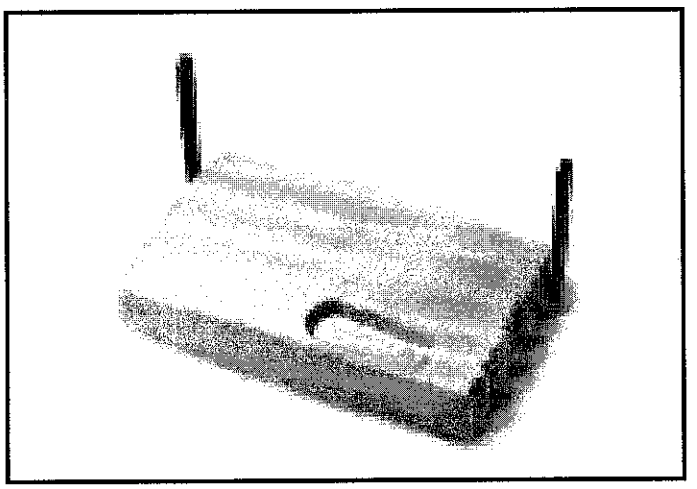


Figure 9 : WLAN Access Point 2221

4.4.4 Baystack 460-24T-PWR

The BayStack 460-24T-PWR Power over Ethernet (PoE) Switch is an IEEE P802.3af draft-compliant switch to power devices such as IP phones, wireless access points, and net cameras. It has 24 10/100 Mbps ports, one MDA (Media Dependent Adapter) slot for uplink connectivity, and one cascade module slot for stacking.

This 10/100 Mbps stackable Ethernet switch is compliant with IEEE P802.3af standard. IP phones or wireless access points from any manufacturer that complies with this standard can be powered from the BayStack 460-24T-PWR. It enables enterprises to power IP devices (IP phones, wireless access points, net cameras) while maintaining connectivity to standard 10/100 Mbps Ethernet devices simultaneously. The BayStack 460-24T-PWR delivers all of the features of the Business Policy Switch such as advanced QoS and high-resiliency with the addition of Power over Ethernet capability. Below shown a model of single Baystack 460-24T-PWR

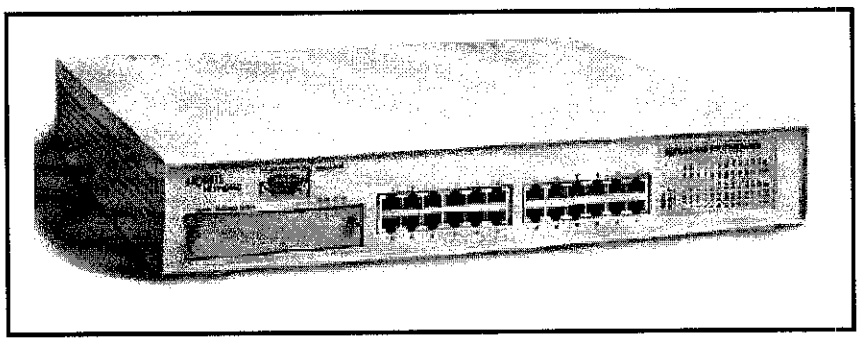


Figure 10 : Baystack 460-24T-PWR

4.4.5 WLAN Security Switch 2250

Nortel Networks WLAN - Security Switch 2250 simplifies management and provides security to the total wireless LAN from a central point. Centralized Security features include Mobile AAA, Global Filters and Mobile Adaptive Tunneling. Centralized Management includes Multiple Authentication Options and MultiService capabilities enabling voice prioritization.

4.4.5.1 WLAN Security Switch 2250 Key features and benefit.

Multi Adaptive Tunneling (MAT) – Provide granular access control to corporate network, enabling administrator to dynamically provide full or limited access to corporate resources based on user profile, access type and device security.
Multiple authenticate options, for the administration to authenticate without the need to duplicate the authentications server.
Robust security, the switch deliver high security features. This enables all traffic to be encrypted using WEP, SSL, IPSec and PPTP as well as support for dynamics session tokens.

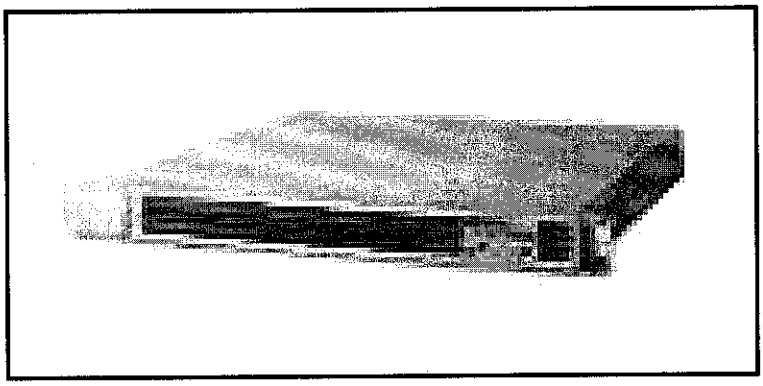


Figure 11 : WLAN Security Switch 2250

4.5 Cost

Price quotation for Nortel Networks 2221 Series meant for 5 access point only (covering the student cafeteria)

PRODUCT DESCRIPTION	QUANTITY	UNIT PRICE (RM)	TOTAL AMOUNT (RM)
Access point	5	8,166	40,830
Wireless Bridge	8	11,314	90,512
Wireless PC Card	20	3,298	65,960
OMNI 6/3 Antenna	5	1,530	7,650
GRAND TOTAL			**204,952**

Figure 12 : Price quotation of WLAN device installation

Price quotation for CISCO AIRONET Series 2 meant for 5 access point only (covering the student cafeteria)

PRODUCT DESCRIPTION	QUANTITY	UNIT PRICE (RM)	TOTAL AMOUNT (RM)
Access point	5	7,345	35,530
Wireless Bridge	8	10,314	88,532
Wireless PC Card	20	2,128	63,940
OMNI 6/3 Antenna	5	1,230	6,640
GRAND TOTAL			**180,356**

Figure 13 : Price quotation of WLAN device installation

The installation of the wireless card should be done step by step in phases. In the preliminary installation, 20 Wireless PC cards will be enough to cater the coverage areas. Adding of the wireless card will be done as the demand grows and the number of potential user increases. As the mobility concerns, every students are recommended to have own laptop or handheld devices.

4.6 WLAN CONCEPTUAL DESIGN

After the completion in determining all the suitable and compatible devices with adheres to standard, the conceptual design will be constructed. The conceptual design will cover the area of Student Center, Student cafeteria and Student Residential. The conceptual design will cater on only in the Village 4 area. However, the same conceptual design also applicable in other students residential including Village 1, 3 and 5. Before allocating the number of access point needed depends upon many different factors including:

i. Area of coverage area
ii. Number of supported users
iii. Network utilization

4.6.1 Coverage Area and Bandwidth.

When designing the layout for the stations, it is very important to note that the distance between the stations directly affects the speed of the network. Table 1 illustrates typical speed in a semi open environment, which is defined as a workspace divided by shoulder height, hollow walls. A station with an 11 Mbps wireless Network Interface card (NIC) can communicate with other client up to a distance of 375 feet (115meters) in a semi open environment. However, only station within the first 165 feet (50 meters) can communicate at 11 Mbps. Station that is between 300 to 375 feet (90 to 115 meters) away will communicate at only 1 Mbps.

DISTANCE BETWEEN STATION (feet)	DISTANCE BETWEEN STATION (meter)	Speed (Mbps)
165	50	11
230	70	5.5
300	90	2
375	115	1

Table 1 : Area of Coverage and Bandwidth

There are certain mode of access point (AP) allocation that need to be determine before setting up the exact location of the access point. Figure 13 illustrate the WLAN environment that uses an access point (infrastructure mode). Infrastructure mode is design where all the station is connected with one or many access point. It capable to cover a larger area since multiple access point is deployed. It is connected in the same wired network.

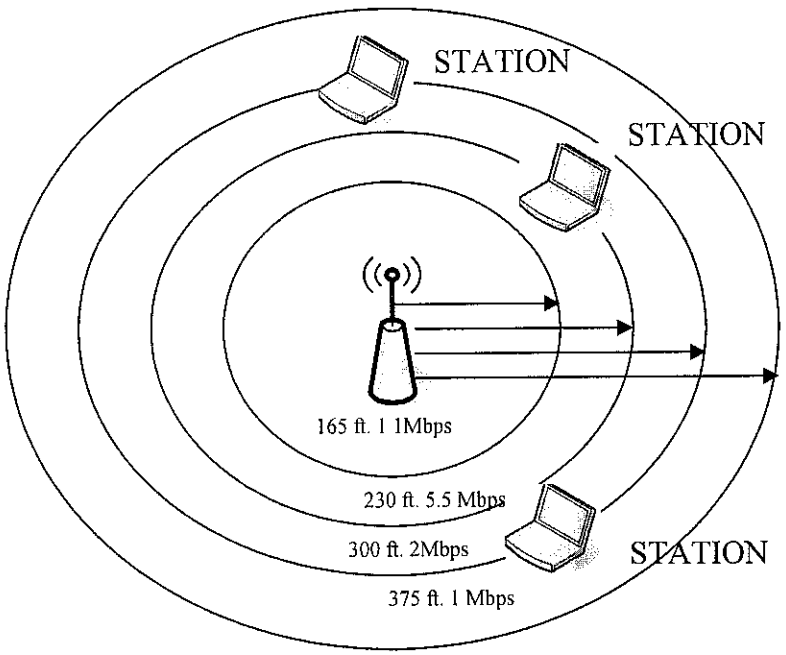


Figure 14 : Bandwidth rate with an access point

A second factor is the number of support red user. A single access point can support between 250 and 300 user in actual practice the number should be fewer. Adding more access point will increase the throughput of the WLAN because fewer user will be contending for access. As shown in Figure 15 is how additional access point can cater number of users.

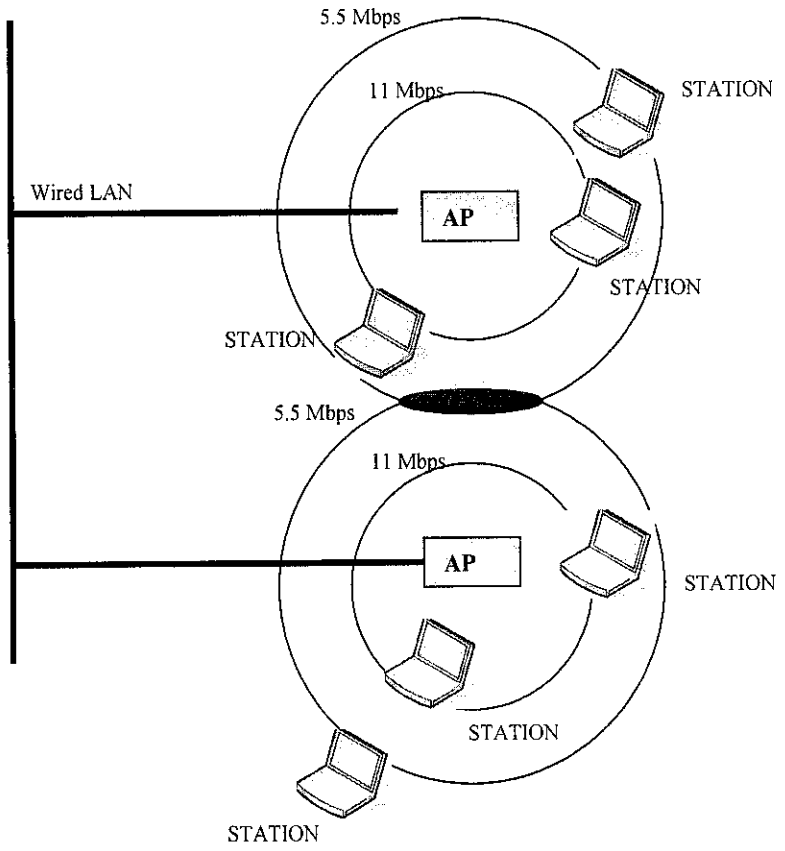


Figure 15 : Additional Access Point.

Student Cafeteria and Student Center including student lounge, launderette, KOPETRO and Student Residential is selected as the area to be shifted to WLAN environment. This is due to this area is semi-open area that cause less interference of signal transmission and low percentage of noise level. Figure 15 shows the access point allocation at the area. Two access points is located at Bay 1 and Bay 2, since this area caters the most students utilizing the WLAN. Based on the site survey result, the cafeteria distance measured approximately 45 meters. These lengths still cater the bandwidth of 11 Mbps. As a result signals can be transmitted at 11 Mbps within this cafeteria area. Based on the result of user density, 55% of UTP student frequently visit the cafeteria. UTP cafeteria can allocate approximately 100 to 150 students at one time. To increase the throughput of WLAN two Access Point (AP) will be allocated in each bay and one Access Point (AP) will be allocated at the Student Center.

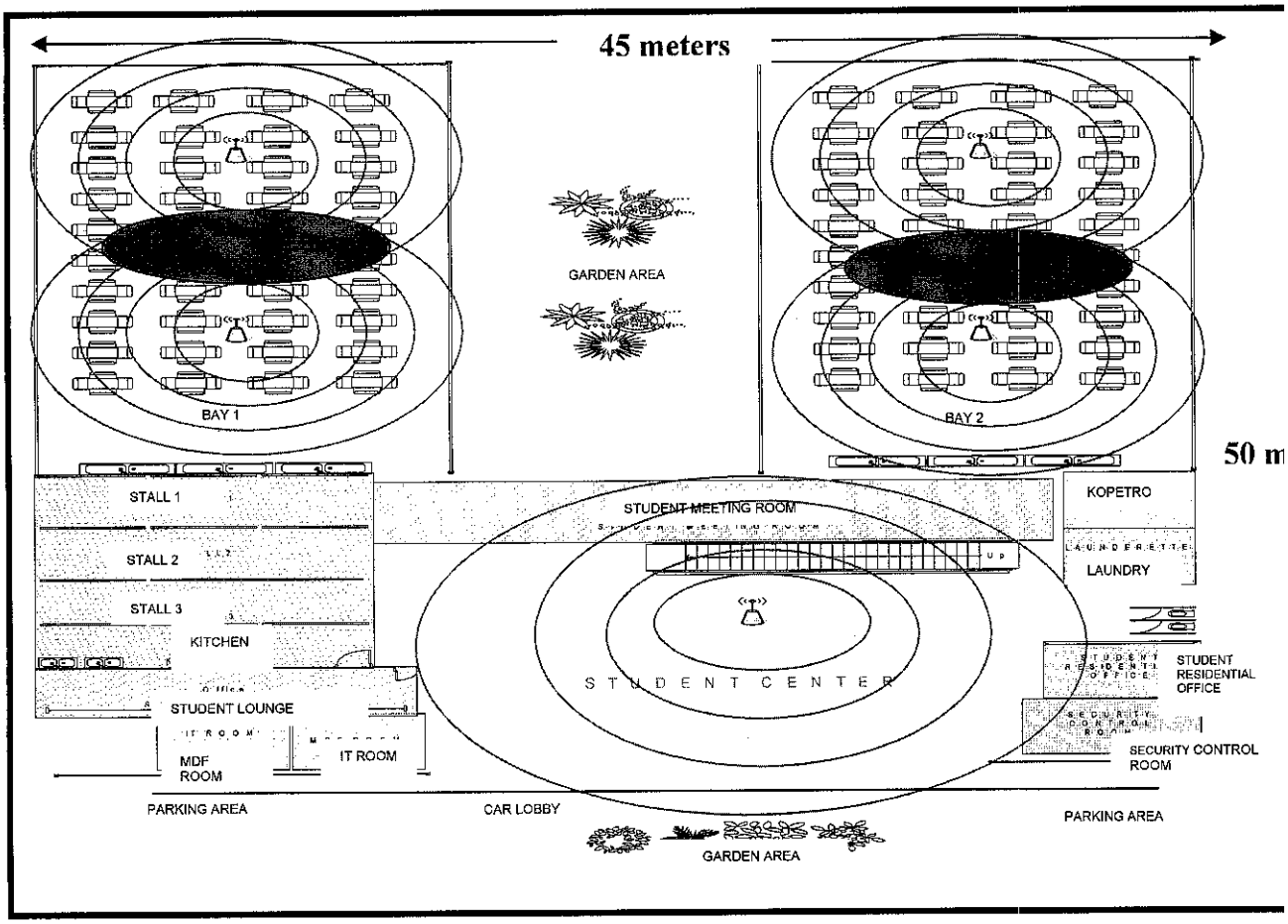


Figure 16 : Access Point (AP) allocation and coverage area in UTP cafeteria.

4.6.2 Conceptual Design and Outdoor Antenna Allocation For whole UTP Cafeteria based on Student Residential (Village 1, 2, 3, and 4)

As shown in Figure 16, are the conceptual designs of devices that will be connected to deploy the WLAN in whole cafeteria area in UTP. In UTP, there are five student residential (Village 1, 2, 3, and 4). Every residential has their own cafeteria, which cater the same number of users at certain period of time. The main Outdoor Antenna (Omni Antenna) will be located at the center of the student residential area, (refer Appendix 1 for exact location of Omni Antenna on UTP map). The Switch (BPS Switch) will route the connection to the Security Access Point (SAPCR) to ensure that the signal transmitted is well secured. The signal will be transmitted and receives through out all the access point (AP) located at the cafeteria area (Bay 1, Bay 2 and Student Center). The DHCP server will determine the Internet Protocol (IP) address of the entire signal based on unique Service Set Identification (SSID) that has been configure through all the access point located at the cafeteria area. The SSID of each access point (AP) in every student residential (Village 1,2,3 and 4) should be unique due to avoid IP conflict.

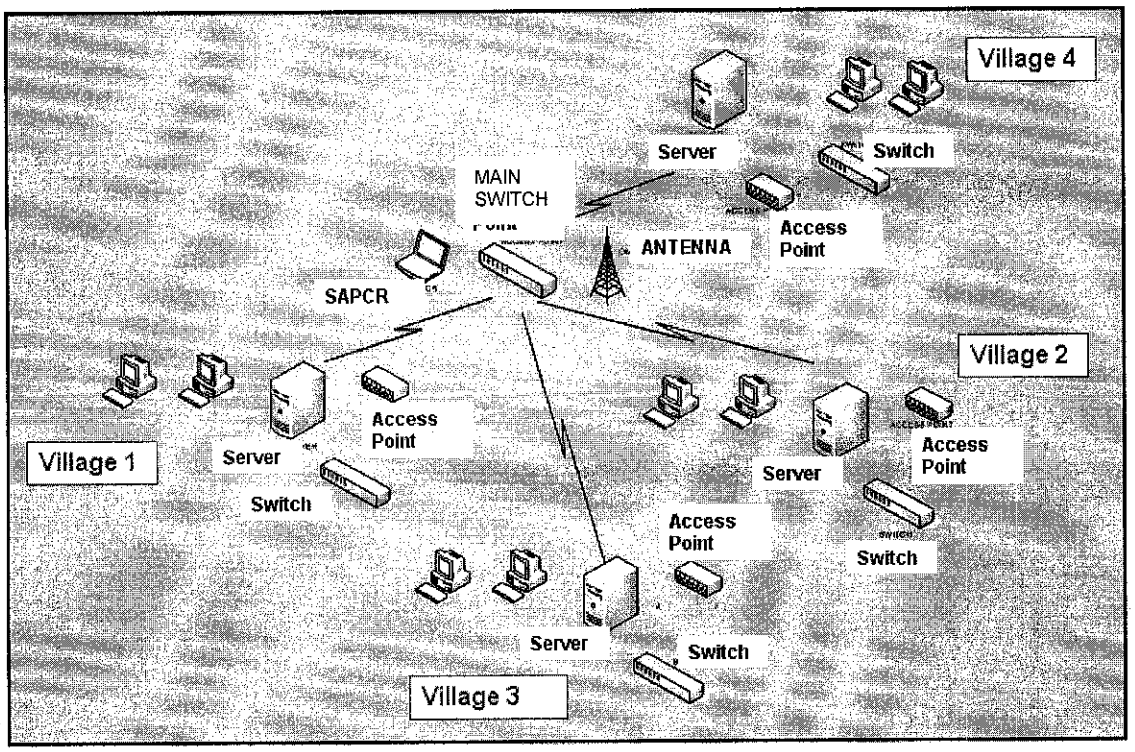


Figure 17 : Conceptual design of whole UTP cafeteria devices setup.

From the previous Figure 16 the conceptual design is more focused on one student residential. Referring to Figure 17, this figure shows us the conceptual design only on Village 4. In UTP every student residential, there are three building (Village 4A, 4B and 4C). The building amount is the same throughout the entire student residential. The same conceptual design is being applied. Every building has their own cafeteria and Student Center. The network routing will be the same as the previous figure described.

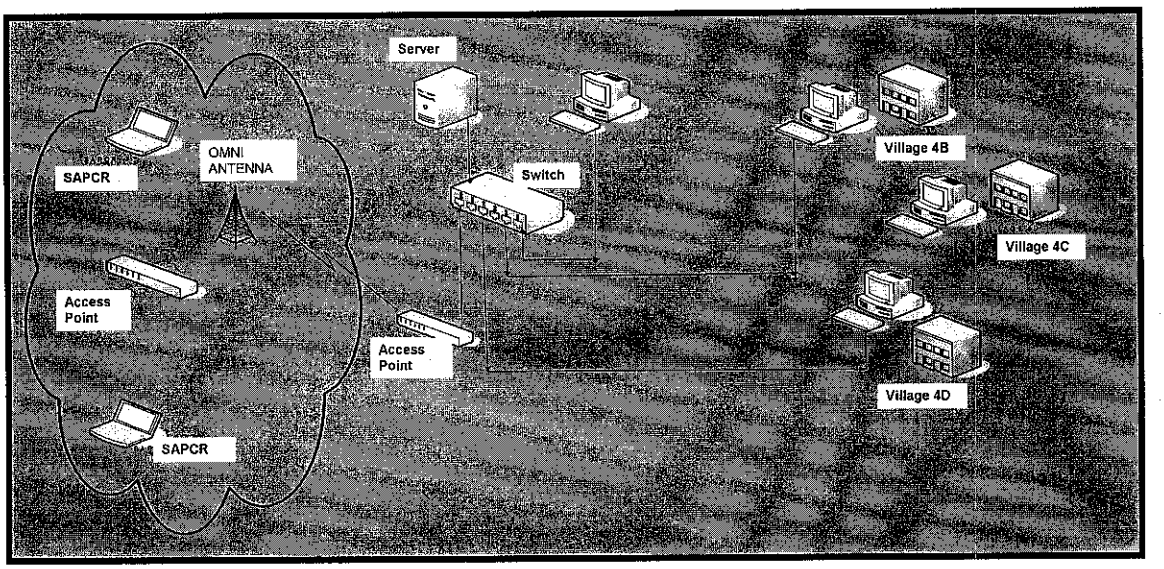


Figure 18 : Conceptual Design focusing on one student residential (Village 4)

4.7 Result and finding stimulation

To gain all the result from the finding, certain stimulations need to be done. The stimulation includes:

i. Site survey
ii. Access Point Setup

This part will include step by step stimulation using all the devices from CISCO AIRONET 350. Noted that this is only a part of demo purposes. The exact devices installation is still being provided by Nortel Network as to secure the cost and device compatibility. The concept of setting the device is more or less the same

4.7.1 Site-survey

Most WLANs have software utility known as a site survey that assists in the placement of access points. It will display such information as the signal level, the outside noise level and signal to noise ratio (SNR) which indicates how much of the signal is being affected by noise. CISCO Aironet 350 also provided their software for this purpose.

Site survey is done by using a laptop on which the site survey software is running, a user roams through the coverage area. A low signal level indicates that the access point may be too far apart. The solution may to relocate or add access points. If noise level is high, user can walk through the area, monitoring the noise level indicator to determine the exact location of the source of interference. Relocating back the access point far from the interferences is crucial.

Figure 11 shows the interface indicating signals bars of every transmission and percentage of beacon received. The CISCO software will also generate and images of the signal strength . This are shown in Figure 12 signal is indicate based on signal strength categorization (Poor, Fair, Good or Excellent)

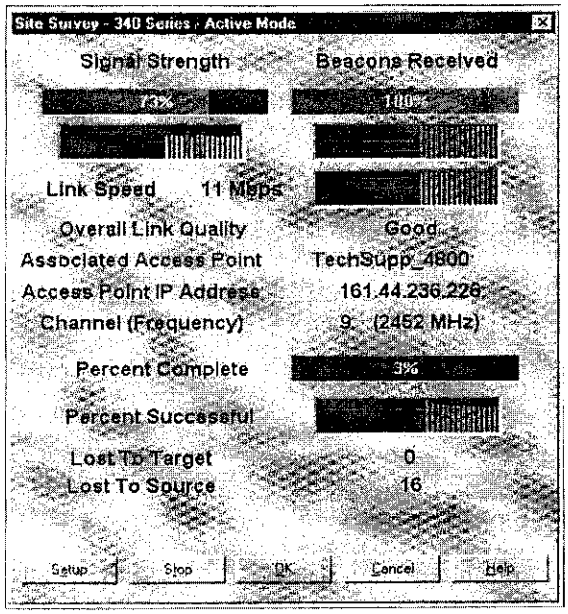


Figure 19 : CISCO Aironet 350 signal indicator by percentage

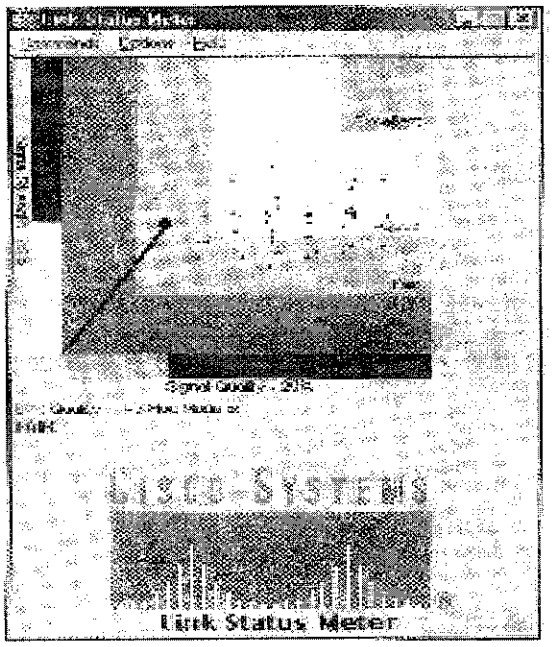


Figure 20 : CISCO Aironet 350 signal indicator by graph

4.7.2 Access Point setup.

i. Primary Port setting

This option will all to designate the bridge radio port as the Primary Port and select whether the bridge primary port is the Ethernet port which is connected to the wired LAN. The primary port setting is set into NO. and for the set the radio port as the primary port (as in demo session the bridge set to IT_AP)

ii. Default IP address

Use this setting to assign an IP for the radio port that is different from the bridge's Ethernet IP address. During the normal operation the radio port adopts the identity of the Ethernet port. When the bridge in standby mode however you assign a different IP address to the radio port.

iii. Service Set ID (SSID)

An SSID is a unique identifier that client devices used to associate with the bridge. SID help client devices distinguish between multiple wireless networks in the same vicinity and provide access ID to VLAN by wireless client devices. Several bridges on a network or sub network can share an SSID.
SSID can be configure to up of 16 SSID on a bridge. It must be an alphanumeric ,case-sensitive from 2 to 32 character long. As for demo purposes SSID set to *datacomm.*
SSID broadcast. This setting is used to broadcast the SSID in search of a bridge to associate with, to associate with the bridge.

CHAPTER 6
CONCLUSION AND RECOMENNDATION

The implementation of the WLAN environment in Universiti Teknologi PETRONAS is only under the planning stages. However, all the equipments and devices has been supplied by the local project contractors and respective consultant from KLCCB Project Berhad and Teliti Computer Sdn. Bhd. The implementation of the WLAN can be done since current LAN setup is already available in UTP campus and under good conditions. The existence of all the core networks at Pocket C, Student Residential (Village 3), and Data Center simplified the shifting to the WLAN by routing all the network connectivity back to the respective server in data center. By considering the entire factor, including the usage model, signal strength, standard adherence, hardware allocation and coverage area, the planning setup for WLAN shifting in UTP campus is fairly justified.

By determining the usage models and peek hours of the WLAN usage is crucial before setting up the Access Point (AP) in the selected area and to determine the number of bandwidth allocated for each user. The surveyed done will help the author in her planning and predicting the capacity of the user using the services and be able to enhance the performance of the services, and to avoid operation run down. As the surveyed concerns, it will help in determining the best cost for all the devices that needed in the setup. As to secure the cost, the author has decided to choose devices provided by Nortel Networks. It is advisable to stay with the current device provider in order to secure the cost of implementation and the compatibility of the operations.

The studies have also been done regarding all the devices involved in the setup to ensure that the capabilities of the devices are compatible with the current LAN setup. Speed of transaction and the signals strength are also the major concern during the installation since it will affect the performance of data transmission will be affected.

Site surveyed is crucial to be done in order to determine the best allocation of all the access point in the selected area and the signal coverage strength and bit of data transmitted per second.

As for further expansion of the work, some new selected areas in UTP campus can be enhanced to adapt the WLAN environment for example, the UTP mosque and Islamic Center, or the New Academic Building areas which include the area of the lecture theaters or other places after considering the usage models and signal strength of each selected area.

REFERENCES

[1] Paul Castro, 2000, *Characterizing Mobility and Network Usage in a Corporate Wireless Local-Area Network*, IBM T.J. Watson Research Center

[2] Anand Balachandran, Geoffrey M. Voelker, Paramvir Bahl, and P. Venkat Rangan. Characterizing user behavior and network performance in a public wireless LAN. In *Proc. of ACM SIGMETRICS'02*.ACM Press, June 2002.

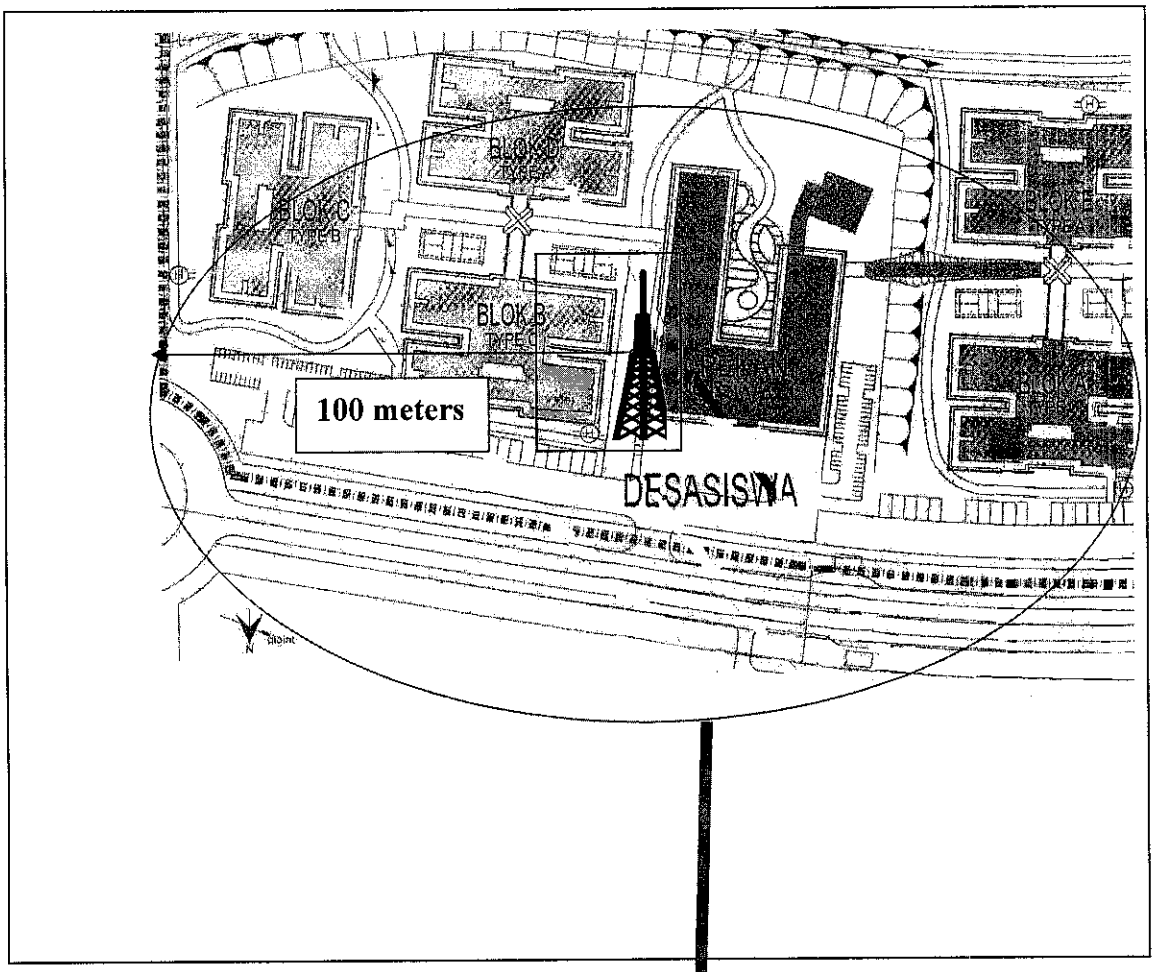
[3] Cisco Systems Inc. Data sheet for Cisco Aironet 350 Series access points. http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/, July 2001.

[4] Anand Balachandran, Paramvir Bahl, and Geoffrey M. Voelker. *Hot-spot congestion relief and user service guarantees in public area wireless networks*. In Proc. of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002). IEEE Computer Society, June 2002.

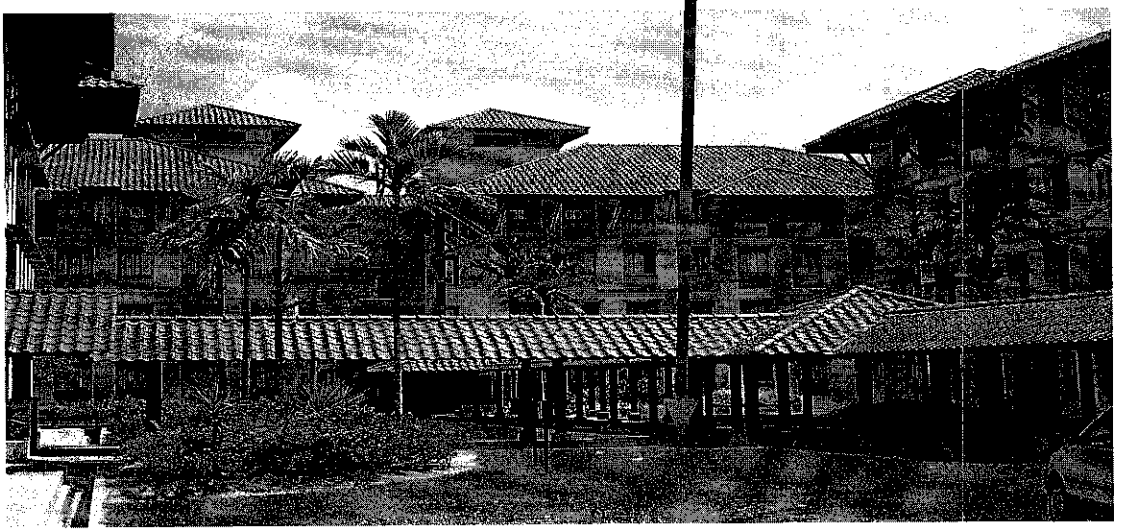
[5] Ann Beheler's , 1999,*Introduction to data communication using CISCO Security,* California,Osborne

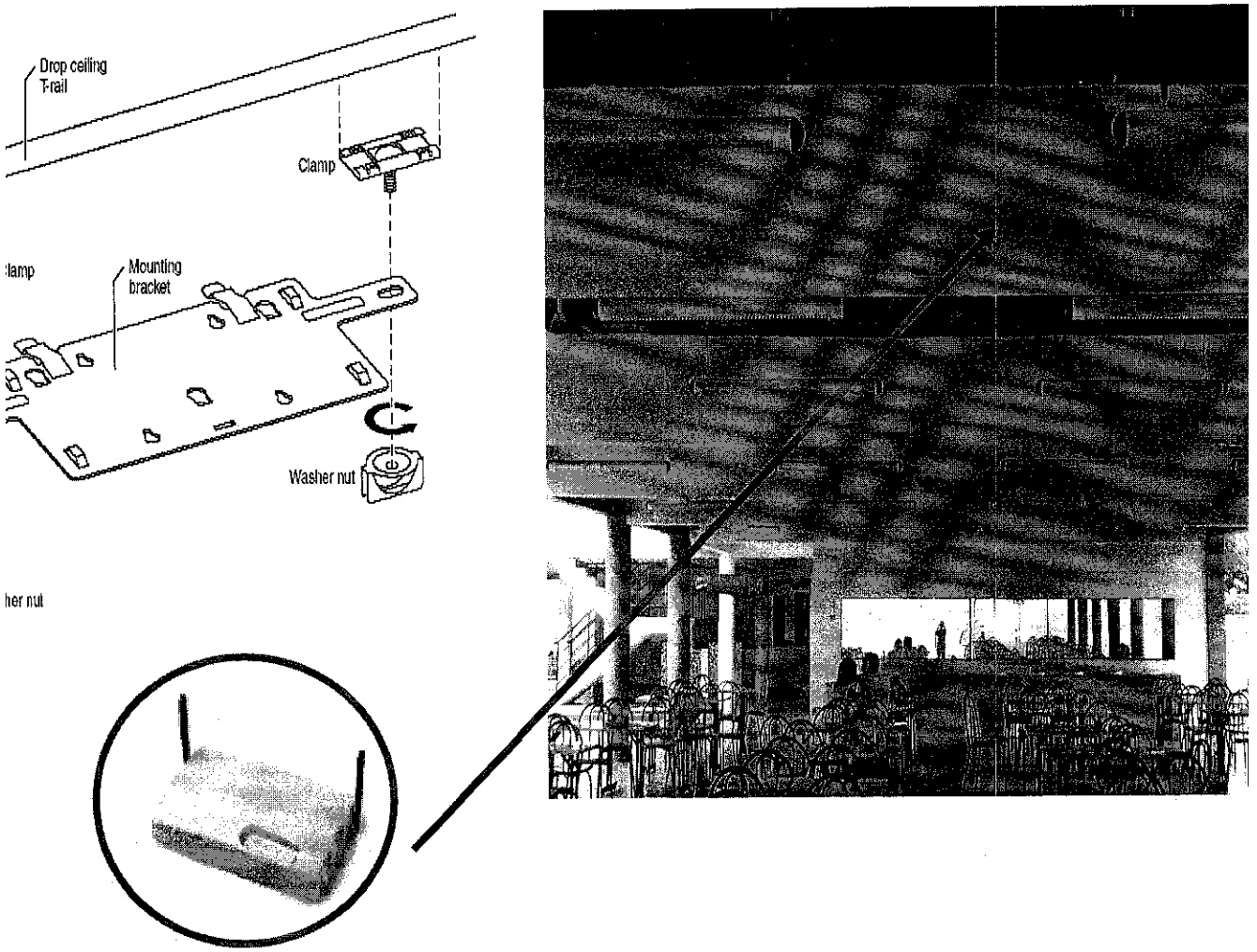
[6] John Hammond 2003, *Wireless HotSpot Deployment Guide*, Intel Communication Inc.

APPENDICES

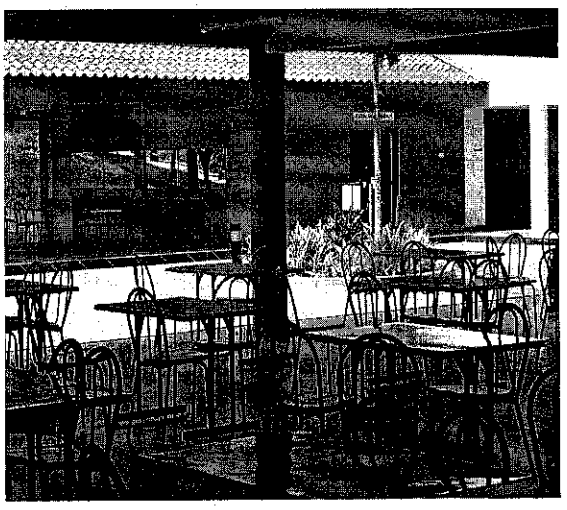


WLAN ANTENNA LOCATION



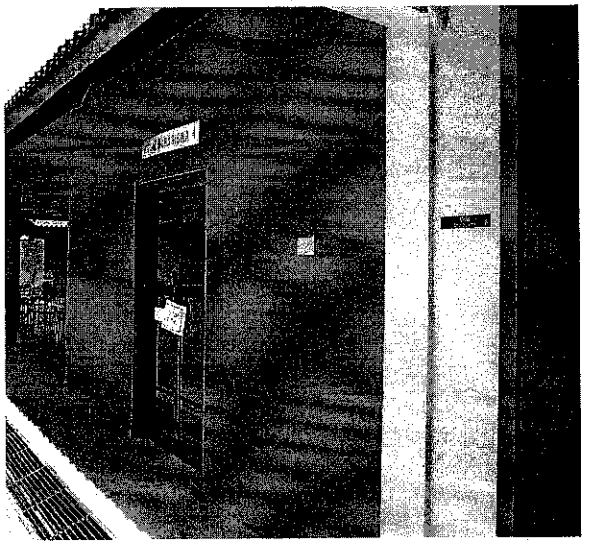


Access Point Claming



DINING AREA BAY 1

STUDENT CENTER



KOPETRO

WLAN COVERAGE AREA IN Universiti Teknologi PETRONAS

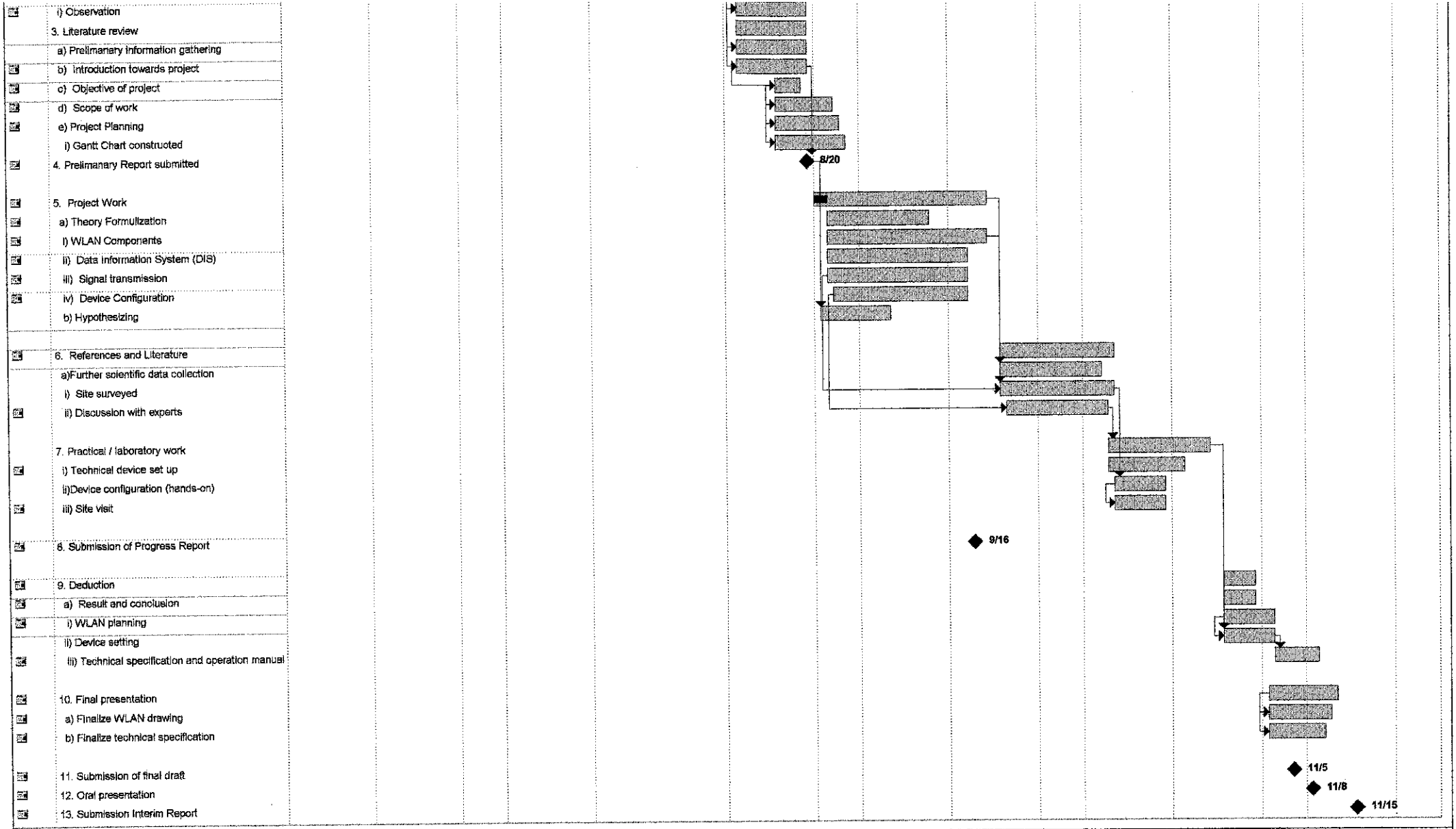
STALL AREA

GARDEN AREA

DINING AREA BAY 2

LIST OF ABBREVIATIONS

- AP Access Point
- CAT5 Category 5
- DHCP Dynamic Host Configuration Protocol
- DES Data Encryption Standard
- DKE Dynamic Key Exchange
- GHz GigaHertz
- HTTP HyperText Transfer Protocol
- HTTPS HTTP Secure
- IEEE Institute of Electrical and Electronics Engineers
- IETF Internet Engineering Task Force
- IPSec Internet Protocol Security
- IRC Internet Relay Chat
- ISP Internet Service Provider
- Kbps Kilobits per second
- LAN Local Area Network
- LEAP Lightweight EAP
- LoS Line of Sight
- MAC Media Access Controller
- Mbps Megabits per second
- MS Mobile Station
- NIC Network Interface Card
- PoE Power over Ethernet
- VLAN Virtual LAN
- VPN Virtual Private Network
- WAN Wide Area Network
- WEP Wired Equivalent Privacy
- WLAN Wireless LAN


i) Observation
3. Literature review
a) Preliminary information gathering
b) Introduction towards project
c) Objective of project
d) Scope of work
e) Project Planning
i) Gantt Chart constructed
4. Preliminary Report submitted
8/20
5. Project Work
a) Theory Formulization
I) WLAN Components
ii) Data Information System (DIS)
iii) Signal transmission
iv) Device Configuration
b) Hypothesizing
6. References and Literature
a)Further scientific data collection
i) Site surveyed
ii) Discussion with experts
7. Practical / laboratory work
i) Technical device set up
ii)Device configuration (hands-on)
iii) Site visit
8. Submission of Progress Report
9/16
9. Deduction
a) Result and conclusion
i) WLAN planning
ii) Device setting
iii) Technical specification and operation manual
10. Final presentation
a) Finalize WLAN drawing
b) Finalize technical specification
11. Submission of final draft
12. Oral presentation
13. Submission Interim Report
11/5
11/8
11/15
Project: tazz
Date: Fri 12/10/04
Task
Split
Progress
Milestone
Summary
Project Summary
External Tasks
External Milestone
Deadline