

IMPLEMENTATION OF WIRELESS LAN IN UTP

by

Nur Zahirah binti Ismail

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

DECEMBER 2004

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

±

TK

5105.7

.A836

N974

2004

1) Local Area Networks (computer networks)
2) wireless communication systems

CERTIFICATION OF APPROVAL

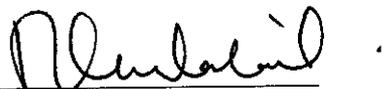
IMPLEMENTATION OF WIRELESS LAN IN UTP

by,

Nur Zahirah Binti Ismail

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

Approved by,


(Mr Khairul Shafee bin Kalid)

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.



NUR ZAHIRAH BINTI ISMAIL

ABSTRACT

This paper, entitled Implementation of Wireless LAN in UTP environment, looks into the way to implement wireless network in UTP. The main objectives of this project are to provide mobile network and internet access using university's network system to students and lecturers and to make it easier and convenient for student to download lecture notes and for lecturers to upload them. Currently, there is no wireless LAN access in UTP environment that can be use by students and staff as alternative opportunity to access and share instant information. Therefore, this project research area is to find out the way to implement wireless LAN using secure Wi-Fi in UTP external environment. For this study, the scope is narrow down to the architecture and design of wireless LAN network and its developing methodology. A network simulation tool called Network Simulator version 2, or simply known as ns-2, is used to test the efficiency and functionality of the designed network. The outcome of this project is a good network architecture design that will give high network performance to all users in UTP.

ACKNOWLEDGEMENT

BISMILLAH AR-RAHMANI AR-RAHEEM

In the Name of Allah, the Most Compassionate, the Most Merciful

I thank GOD who gave me the spirit and strength to work and proceed with this project, going through all the problems and finally able to deliver it.

My sincerest thanks go to my supervisor, Mr. Khairul Shafee bin Kalid. Thanks for his supports, patience and ideas in assisting me with this project, his never-ending enthusiasm inspires me.

I also would like to express my gratitude to staff of Universiti Teknologi PETRONAS, especially IT IS committee and lecturers for providing knowledge and resources and willing to help with full commitment. Your supports and commitments really help me.

Special thanks to my housemates, colleagues, and friends for helping me with this project and for always be at my side whenever I need the helps. Thanks for the courage, the passion and the friendships we shared together.

Credits to those who help and guide me on my project via Internet. Thanks for spending their precious time answering all my questions.

Last but not least, deepest gratitude to my parents and family for their enormous material and spiritual supports, without them this work would not have been possible.

TABLE OF CONTENTS

ABSTRACT	i
CHAPTER 1: INTRODUCTION	1
1.1 Background of Study	1
1.2 Problem Statements	1
1.2.1 Problem Identification	1
1.2.2 Significant of the Project	2
1.3 Objectives and Scope of Study	2
CHAPTER 2: LITERATURE REVIEW	4
2.1 Introduction	4
2.2 Wireless LAN Standards	5
2.2.1 Wireless LAN Standard in UTP.	7
2.3 Wireless Network Architecture and Design	8
2.3.1 Wireless LAN Secure Architecture	9
2.3.2 Wireless Access Point Placement	11
2.4 Benefits of Wireless LAN	13
2.5 Case Studies	15
2.5.1 A Technology College in London	15
2.5.2 Harvard Medical School	16
2.5.3 Toyohashi University of Technology	19
CHAPTER 3: METHODOLOGY	21
3.1 Procedure Identification	21
3.1.1 Information Gathering and Fact-Finding	22
3.1.2 Design	22

	3.1.3	Simulation	22
	3.1.4	Result	23
	3.2	Tools Required	24
CHAPTER 4:		RESULTS AND DISCUSSION	26
	4.1	Findings	26
		4.1.1	General Findings	26
		4.1.2	Existing UTP Network Architecture	26
		4.1.3	Proposed UTP Network Architecture	30
		4.1.4	Simulation Result	33
		4.1.5	Conclusion from the Simulation	45
	4.2	Discussions	46
		4.2.1	Wireless Environment.	46
		4.2.2	Simulation Results	47
CHAPTER 5:		RECOMMENDATION & CONCLUSION	48
	5.1	Recommendation	48
	5.2	Conclusion	49
REFERENCES			51
APPENDICES			54
		APPENDIX A: HARVARD MEDICAL SCHOOL (HMS) WIRELESS		
		QUAD LOCATIONS		55
		APPENDIX B: WIRELESS NETWORK DEVICES AND PRICES		56
		APPENDIX C: WIRELESS LAN CONFIGURATION TO PC AND PDA		57

APPENDIX D: NETWORK SIMULATION V2 CODING	67
APPENDIX E: INTRODUCTION TO NETWORK SIMULATOR (NS) VER. 2	73
APPENDIX F: PROJECT SCHEDULE	83
APPENDIX G: GLOSSARY	84

LIST OF FIGURES

- Figure 2.1 Typical wireless LAN architecture
- Figure 2.2 An example of Virtual LAN architecture
- Figure 2.3 An example of Virtual Private Network (VPN) architecture
- Figure 2.4 An example of AP placement
- Figure 2.5 GW-AP110 placements in the building as proposed by Planex Communication Inc
- Figure 3.1 Custom Methodology used in this Project
- Figure 3.2 Example of an access point (AP)
- Figure 3.3 Example of PCMCIA wireless network card
- Figure 3.4 Example of PCI wireless network card
- Figure 4.1 UTP Current Network Diagram
- Figure 4.2 Library Current Network Diagram
- Figure 4.3 Building 1 and 2 ground floor layout
- Figure 4.4 Building 1 and 2 first floor layout
- Figure 4.5 Building 1 and 2 second floor layout
- Figure 4.6 Building 1 and 2 third floor layout
- Figure 4.7 Proposed Wireless Network at Library
- Figure 4.8 Proposed Wireless Network at Building 1 and 2 of Academic Complex
- Figure 4.9 Wireless Hardware Setup Diagram
- Figure 4.10 Simplified User's View of NS
- Figure 4.11 Nodes start to move to their destination at time 0.0s
- Figure 4.12 Wireless signal starts and node 1 start send packets at time 3.0s
- Figure 4.13 Packets drop as nodes move away
- Figure 4.14 Packet drops after reaching stop time, 25.0s
- Figure A-1 The HMS Wireless Quad Locations
- Figure C-1 "Network Connections" icon

- Figure C-2 “Wireless Network Connection” icon
- Figure C-3 “Wireless Network Connection Properties” window
- Figure C-4 “Wireless Network Properties” window
- Figure C-5 “Authentication” tab under “Wireless Network Properties” window
- Figure C-6 “Internet Protocol (TCP/IP)” menu
- Figure C-7 “Internet Protocol (TCP/IP) Properties” window
- Figure C-8 “Advanced TCP/IP Settings” window
- Figure C-9 “Connections” tab under “Internet Properties” window
- Figure C-10 “Local Area Network (LAN) Settings” window
- Figure C-11 Toshiba e740 Pocket PC with built-in wireless capabilities configuration
- Figure C-12 Wireless Configuration Menu
- Figure C-13 “Profile” window
- Figure C-14 Menu window
- Figure C-15 “Network Preferences” drop down menu
- Figure C-16 “New Service” properties
- Figure C-17 “Service Connection Progress” prompt window
- Figure C-18 “Login Confirmation” window
- Figure C-19 Browser window
- Figure F-1 Project Schedule

LIST OF TABLES

Table 2.1	Wireless IEEE Standard Comparison
Table 4.1	Parameters defined in the simulation
Table 4.2	Nodes start positions
Table 4.3	Values defined for node movement
Table 4.4	Start time of sending packet for each node
Table B-1	Wireless Devices and Price List

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND OF STUDY

Wireless LAN (WLAN) provides wireless network communication over short distances using radio or infrared signals instead of traditional network cabling. A WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter similar in function to a traditional Ethernet adapter. For this project, Wi-Fi technology will be used to implement this WLAN network environment. Security measures will also be implemented in the WLAN area. One issue in the design and implementation of a wireless local area network is the selection of access point (AP) locations. Some review on the architecture of WLAN and its network design is done so that a good network design could be produced by the end of this project. A suitable network simulation tool will be used to test the efficiency and functionality of the designed network.

1.2 PROBLEM STATEMENT

1.2.1 Problem Identification

Currently, students might not get the latest information from the lecturer should the class suddenly be cancelled. Therefore, by implementing WLAN access in UTP environment using secure Wi-Fi, both students and staff can use this convenient facility as an alternative opportunity to access online information at anytime. The reason for implementing WLAN is its simplicity to be set up and connecting computers from anywhere with less wire needed. Students found that sharing latest information is

impossible if instant network connection is not available when needed. With WLAN, users can access shared information without need to look for plugs and network managers can set up or augment networks without installing or moving wires especially when working in a temporary office. WLAN could extend network to every square inch of buildings, campus or residence without the physical limitations of wires or cables so that a network connection could be established.

1.2.2 Significant of the Project

The solution for this project is to find out the WLAN architecture and its methodology for implementing the wireless network. This is to find out the needs and also the steps taken to develop a WLAN. WLAN can also be configured in a variety of topologies to meet the needs of specific applications and installation as the configuration is easy to change. It limits the amount of cabling and labor associated with installation and as result, the cost to install and maintain the network is lower than wired LAN.

This project is limited to be implemented in UTP environment only. As WLAN is relatively simple to reconfigure and expand, UTP can reduce the nature cost of WLAN including the indirect cost resulting from user downtime and administrative overhead. It will also be a convenient facility to student and staff in UTP.

1.3 OBJECTIVES AND SCOPE OF STUDY

The main objective of this project is to provide convenient mobile network and Internet access using university's network system to students and lecturers. It is also to make it easier for student to download lecture notes and for lecturers to upload them at anytime and anywhere they want.

Second objective of this project is to reduce the nature cost in implementation of wireless such as cost of ownership, maintenance and installation. Long-term cost benefits are greatest in dynamic environments requiring frequent move, additions and changes to the existing network.

Lastly, this project will produce network architecture and design that is suitable for UTP from the simulation done using an object-oriented simulator called Network Simulator version 2 (ns-2). This project will also suggest some methodology to implement the network so that clear view of networking is achieved and optimal network service could be obtained.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

Wireless LAN is a local area network that transmits over the air typically in an unlicensed atmosphere such as the 2.4GHz band. According to Yasmin (1999), WLAN refers to a wireless network between computers within one building or a group of buildings to enable sharing of resources and to interconnect various organizations.

Webopedia (2004) stated that most LANs connect workstations and personal computers and each node (individual computer) in a LAN has its own CPU with which it executes program, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions. There are enormous needs for more flexible LAN as on the go access for information such as file sharing, Intranet and Internet have widely spread. WLAN increased mobility as it enables better communication, enhances productivity and enables better customer service. A WLAN allows users to access information beyond their desk, and conduct business anywhere within their offices.

Besides, WLAN could reduce the cost of ownership as the initial cost of implementation is lower than traditional networks. The longer term benefits are highest in environments where there are frequent network moves, changes and, or additions.

Finally, WLAN increased flexibility because it is well suited to many environments. As an extension to a wired network, it allows access anywhere within buildings. For difficult to cable locations such as heritage buildings or sites where new wiring cannot be laid for structural reasons, wireless is ideal. Wireless makes sense for temporary office connectivity (SWL, www.simplywirelesslan.com).

Wireless network has become a new trend to today's world. Modern business requires mobility and always-on connectivity to compete. Cell phones and PDAs have become indispensable for business. Barthold (2004) reports that wireless networks such as 3G (third-generation) cellular, Wi-Fi and even WiMAX, will eventually overlap to blanket enterprises and business campuses with easy-to-use, high-speed data and voice connectivity through a device that looks like today's cell phone.

Dave Juitt (quoted by Barthold), CTO of Bluesocket said that devices used nowadays such as cell phones are going to have to be smart enough to know what network it's connected to. Meanwhile, Joel Short, CTO and senior vice president of Nomadix said that gathering places like airports, hotels and convention centers "have to have Wi-Fi". This will provide easy access to network from anywhere at anytime.

2.2 WIRELESS LAN STANDARDS

The WLAN standards were started with the 802.11 standard, developed in 1997 by the IEEE. This base standard allowed data transmission of up to 2 Mbps. Over time, this standard has been enhanced. According to Michael, there are a few different wireless standards such as 802.11a, 802.11b and 802.11b/g that are categorized as first generation, and 802.11d, 802.11e, 802.11f, 802.11g, 802.11h, 802.11i and 802.11x that are the second generation. Table 1 shows the details of currently used standards. (Quoted by James Kaczman)

IEEE Standard	Data Rate	Modulation Scheme	Security	Pros/Cons
802.11	Up to 2Mbps in the 2.4GHz band	FHSS or DSSS	WEP & WPA	This specification has been extended into 802.11b.

802.11a	Up to 54Mbps in the 5GHz band	OFDM	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." Eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b. Not interoperable with 802.11b.
802.11b	Up to 11Mbps in the 2.4GHz band	DSSS with CCK	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." Not interoperable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high-speed access to data at up to 300 feet from base station. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
802.11g	Up to 54Mbps in the 2.4GHz band	OFDM above 20Mbps, DSSS with CCK below 20Mbps	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." May replace 802.11b. Improved security enhancements over 802.11. Compatible with 802.11b. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.

Table 2.1: Wireless IEEE Standard Comparison

Other standards such as 802.11d and above are still new and not been used widely. From IEEE article on IEEE 802 General Information, IEEE 802.11e is the first wireless

standard that spans home and business environments. It adds quality-of-service (QoS) features and multimedia support to the existing IEEE 802.11b and IEEE 802.11a wireless standards, while maintaining full backward compatibility with these standards. QoS and multimedia support are critical to wireless home networks where voice, video and audio will be delivered. Broadband service providers view QoS and multimedia-capable home networks as an essential ingredient to offering residential customers video on demand, audio on demand, voice over IP and high-speed Internet access.

This article also wrote that IEEE 802.11i standard adds the Advanced Encryption Standard (AES) security protocol to the 802.11 standard for wireless LANs. Security has been a primary concern for IT managers reluctant to deploy wireless networks, but AES is a stronger level of security than found in the current Wi-Fi Protected Access security standard.

From Nortel Networks paper, it wrote that IEEE 802.11f standard is a “recommended practice” document that aims to achieve AP interoperability within multivendor WLAN network by defining a common IAPP. As addition, IEEE 802.11h is a supplementary 802.11 standard to comply with European regulations for 5GHz WLANs limiting transmit power and selecting the channel for lowest interference with other system such as radar. Finally, the IEEE 802.1x provides authentication or access control for the APs through the use of the Extensible Authentication Protocol (EAP), which is a set of messages for authentication negotiation and authentication transport method between client and server.

2.2.1 WLAN Standard that will be used in UTP

Among all IEEE standards that are existed, 802.11g is more suitable to be used in UTP network environment. It offers the same 54 Mbps of throughput like 802.11a do, which is useful for applications such as voice over WLAN and mobile videoconferencing. The main advantage of 802.11g over 802.11a is that it operates in the 2.4 GHz band and was designed to be backwards compatible with 802.11b, which is suitable for checking e-mail and accessing presentations, documents, and the Web. 802.11g is the best standard to be used as these applications are most applied by UTP students. The main problem

with 802.11g is that it still occupies that crowded 2.4 GHz band, which must share space with such devices as microwaves and cordless phones.

2.3 WIRELESS NETWORK ARCHITECTURE AND DESIGN

WLAN uses electromagnetic airwaves (radio or infrared) to communicate information from one point to another without relying on any physical connection. Article from Nouveau Solution Limited wrote that radio waves are often referred to as radio carriers because it simply performs the function of delivering energy to a remote server. Multiple radio carriers can exist in the same time without interfering with each other if the radio waves are transmitted on different radio frequency. A radio receiver tunes in one radio frequency while rejecting all other frequency to extract data. Figure 2.1 below shows a typical wireless LAN network architecture.

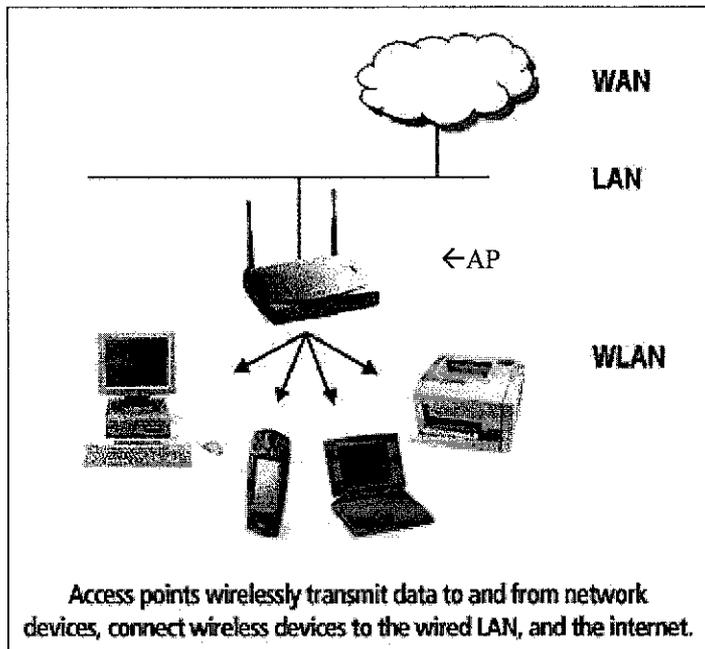


Figure 2.1: Typical wireless LAN architecture

Yasmin reported that a typical WLAN configuration, a transmitter and receiver (transceiver) device, called an access point (AP), connects to the wired network from a fixed location using standard cabling. Finding the optimal locations for AP is important for its performance, and can be achieved by measuring the relative signal strength of the

AP. Placing the AP in a corporation network opens an access way to the resources in the Intranet. The obvious way to extend the Intranet with a WLAN is to connect the AP directly to it.

2.3.1 Wireless LAN Secure Architecture

Dave (1999) wrote that the terminals that wish to join the wireless network need to know the SSID (Service Set Identifier) string that identifies the network. When the terminal enters the coverage area of an AP in that network, it can start associating with an AP. The authentication methods supported by the current 802.11 standard are Open System and Shared Key. The Shared Key method requires that the WEP algorithm be implemented on both the wireless terminal and the AP. In the Open System authentication scheme, which is the default scheme, a terminal announces that it wishes to associate with an AP, and typically the AP allows the association. To restrict access to a wireless network without WEP, most WLAN product vendors have implemented an access control method, which is based on blocking associations from unwanted MAC addresses on the AP.

If no authentication or encryption methods are used, the WLAN can create a security risk in case the radio signals flow outside the office building. To prevent eavesdropping and unauthorized access to the WLAN, other security measures should be implemented if the transmitted data is valuable to the business. According to Scholz (2002), there are varieties of options available for building and securing wireless networks, regardless of whether all options are implemented. The security inherent with IEEE 802.11 wireless networks is weak at best. The 802.11 standard provides only for Wired Equivalent Privacy (WEP), which was never intended to provide a high level of security. He also added that, wireless networks can be highly secure by using a combination of traditional security measures, open standard wireless security features, and proprietary features.

From this article, Scholz mentioned that security is grouped into two areas, which are maintaining confidentiality of traffic on the wireless network and restricting use of the wireless network. It is also assumed that security-related services such as authentication

servers and firewall devices are available on the wired network to control the wireless network traffic. A wireless network hacker does not need to be present in the facility. All that is required to intercept wireless network communications is to be within range of a wireless access point inside or outside the facility. In a highly secure environment, a best practice is to have the wireless access points connect to a wired network physically or logically separate from the existing user network. This is accomplished using a separate switched network as the wireless backbone or with a *Virtual LAN (VLAN)* that does not have a routing interface to pass its traffic to the existing wired network. Figure 2.2 shows an example of a Virtual LAN.

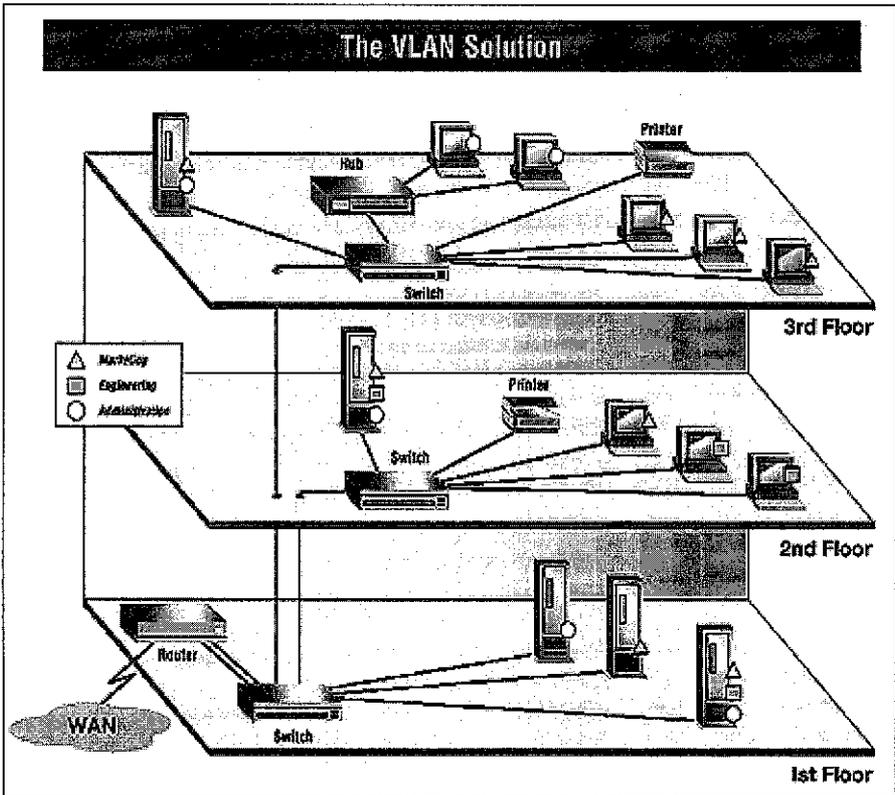


Figure 2.2: An example of Virtual LAN architecture

This network terminates at a *Virtual Private Network (VPN)* device, which resides behind a firewall. In this way, traffic to and from the wireless network is controlled by the firewall policy and, if available, filters on the VPN device. The VPN device will not allow any traffic that is not sent through an encrypted tunnel to pass through, with the

exception of directed authentication traffic. Shown in Figure 2.3 below is example of VPN architecture.

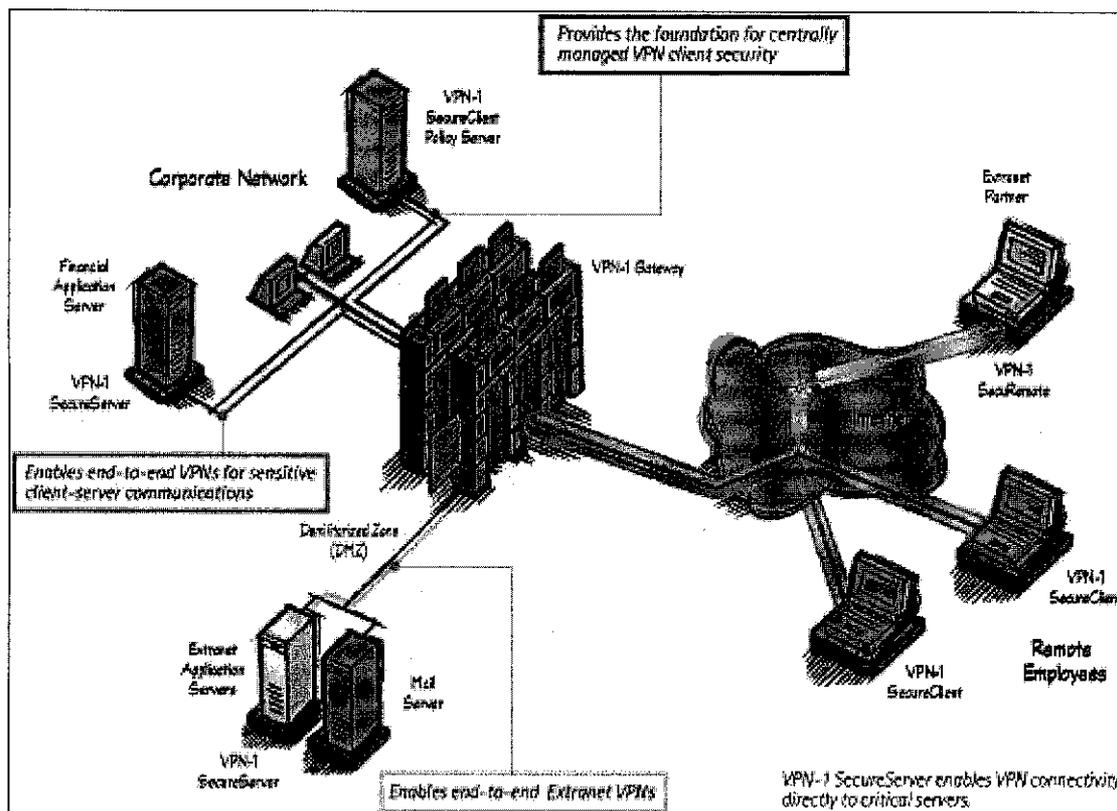


Figure 2.3: An example of Virtual Private Network (VPN) architecture

2.3.2 Wireless Access Point Placement

The placement of access points (APs) is very important to build an efficient wireless network. This is to ensure that the network will perform at it best. One issue in the design and implementation of a wireless local area network is the selection of AP locations. Proper AP placement is necessary to provide adequate signal coverage and also to minimize co-channel coverage overlap. The impact of incorrect placement of APs is significant. Placing APs too far apart can lead to gaps in coverage. On the other hand, placing the units too close together leads to excessive co-channel coverage overlap, degrading system performance (Alex, Ben & Jon, 2004). Figure 2.4 shows an example of AP placement.

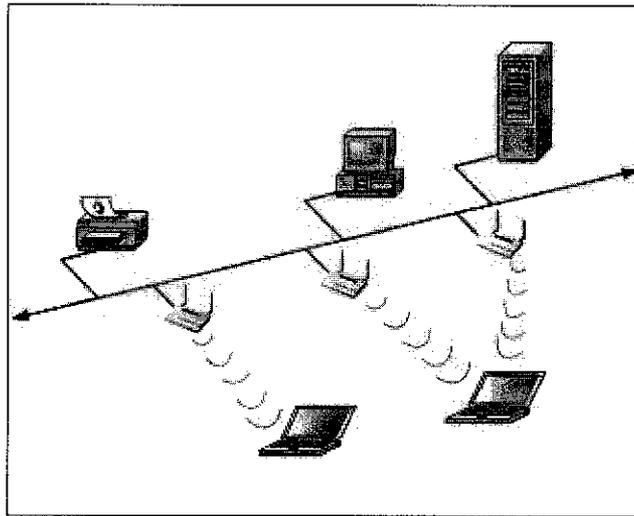


Figure 2.4: An example of AP placement

Some factors that need to be considering when implementing a wireless network, especially when placing the AP, are the geographical and physical around the area. This is because the frequency of signal could become low due to the physical factor such as wall blocking and the material used such as steel at the cubicles that will block the signal from reaching the client. According to Del Smith (2003), an overlapping AP's transmission radius, called a cell, using multiple access points creates seamless access as user roam from one cell to another. He also added that the size of cell will depends largely on two factors, which are the type of 802.11 used and possible obstacles and interference that the radio frequency (RF) signal may encounter. The number and placement of clients could be made to ensure the strength of wireless signal. Del Smith wrote that adjustment of number and placement of clients could be done based on the equipment selected and its configuration. At this point, adjustment may be done by referring to the number of cells required to provide coverage for heavily occupied areas, such as cubicle clusters and conference rooms.

Area that did not have any blocking from obstacles will have a high signal even if the user is quite far from the AP. Del Smith wrote that radio frequency is susceptible to signal loss resulting from the materials it has to pass through, known as attenuation. Typical office obstacles such as doors, windows, walls, and furniture result in attenuation. This attenuation is in addition to the path loss resulting from simple range

traveled between endpoints. As addition, Mitchell (2004) wrote that the wireless equipment placement should avoid reflective surfaces whenever possible as Wi-Fi signals literally bounce off of windows, mirrors, or stainless steel countertops, which will result in lessening both network range and performance.

Other factor such as interference from other organization's signal that are stronger than signal being used by an organization, will make the signal from the AP disappeared. Del Smith added that because of the 802.11 medium access protocol, an interfering RF signal of sufficient amplitude and frequency can appear as a bogus 802.11 station transmitting a packet. This causes legitimate 802.11 stations to wait for indefinite periods of time until the interfering signal goes away. Depending on the environment, this may or may not be a problem during the planning stage. For 802.11a and 802.11g wireless LANs, microwave ovens, wireless phones, Bluetooth-enabled devices, and other wireless LANs can cause problems. He added that the use of a spectrum analyzer will provide a detailed report of possible interference.

If the best location found was only marginally acceptable, consider adjusting the base station antennas to improve performance. Antennas on wireless access points and routers can usually be rotated or otherwise re-pointed to "fine tune" Wi-Fi signaling. For best results, follow the specific manufacturer's recommendations. There are also some alternatives, to ensure the optimal performance of WLAN where user could replace and upgrade the base station antennas or install a Wi-Fi repeater, which is often called a "range extender" or "signal booster." Finally, in extreme cases, user may need to configure a second base station to extend the range of WLAN.

2.4 BENEFITS OF WIRELESS LAN

WLAN is known as a network that interconnects computers for information sharing within the same building without wire. As said by Yasmin, by using wireless connections, it allows portable computers to still be portable without sacrificing the advantages of being connected to a network. Furthermore, the increased use of mobile phones and Personal Digital Assistant (PDA) devices is driving the workforce towards a

more mobile working environment. This shows that WLAN is highly mobility as it can provide network users with access to real-time information anywhere in organization. Besides, the installation could be done faster and easy as it eliminates the need to pull cable through wall and ceilings.

As addition, while the initial investment required for WLAN hardware can be higher than wired LAN, overall installation expenses and life-cycle costs can be significantly lower. SWL stated that Long-term cost benefits are greatest in dynamic environments requiring frequent move, additions and changes. Besides, WLAN is also flexible as the rapid transition time from one configuration to another that wireless provides can help reduce network downtime (Stone, 2004).

WLAN also can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users, allowing for roaming over broad area. In accordance with SWL, hotspots are being deployed in many public places worldwide and to connect to a hotspot a wirelessly enabled laptop or handheld is needed. Wireless Fidelity (Wi-Fi), which means unprecedented freedom for users, makes it easier to be connected when traveling world wide.

From the case study that have been done, it shows that these benefits are proven and true as some of the institution that had implement wireless LAN network found it is beneficial to their organization. As reported by BlueSocket Inc., Harvard Medical School shows that authenticating users, not devices, has proved to be a prudent policy/approach as students and faculty may seek access to servers from a variety of devices and from a variety of locations. It is also written that when a Harvard Medical student wants to travel to Harvard Yard in Cambridge and conduct research at either the Widener or Cabot Science Libraries, they can just turn on their laptop and get connected. As addition, a former network analyst who worked on the project said that Bluesocket's open and non-proprietary approach addresses the fact that students and faculty alike may go between several different wireless networks within the same day.

Other benefit includes HMS made their entire curriculum available online so that the students could access it virtually by using PDAs and wireless access, working and studying wirelessly enhances collaboration among students and fosters improved interaction between students and faculty, its flexibility as students could use it whenever and wherever they want to as the wireless goes hand-in-hand with in-dorm high speed wired access, mobility in medicine where the students able to access information at any time they want. It also improves research conducting by their students as they can use their laptop to search for resources from one of the great medical libraries.

2.5 CASE STUDIES

2.5.1 A Technology College in London

Centre for Engineering and Manufacturing Excellence (CEME), set up in East London by motor manufacturer Ford in conjunction with local development agencies and colleges, has been given the opportunity to build a state-of-the art network from scratch at a new technology college. The first principles taken into account by the team were:

- The college needed to offer anywhere-access to up to 1,200 students internally and a greater number logging in from outside the campus
- The IT strategy needed to be aligned to business needs so that money saved could be reinvested
- The network needed to be highly secure and scalable up to 50,000 users.

The college will make heavy use of IP telephony and wireless networks to allow access from anywhere, voice and video over the network and hot-desking in the college. All this will run on Microsoft infrastructure and applications on IBM hardware linked via Cisco Avvid voice, video and data network technology supplied by Omnetica.

Students and lecturers increasingly expect to be able to use mobile devices, such as portable computers and Tablet PCs, wherever they are working, teaching and learning. CEME is backing this requirement with wireless LAN support and making Tablet PCs and portable computers available to students and lecturers. This would mean that a

student could sit in a lecture taking notes on a Tablet PC, simultaneously checking background information on the subject from the information portal.

The provision of state-of-the-art e-learning facilities is an important goal for CEME, so the centre needed networks, software and hardware that could provide facilities such as real-time video and multimedia lectures. CEME needs to be able to deliver E-learning functionality in a stable, low management and virtually transparent way.

As a training facility for future engineers, CEME is also ensuring it operates in an enterprise culture from the start. This is evident in the considerations taken into account in planning the network infrastructure. The team worked rigorously with their stakeholders and business partners to align our IT strategy to their business strategies and to ensure that IT is a business-driven line activity and decisions were based on value.

The advantages that they get by implementing wireless network in the organization includes the ability to access college information from anywhere they want, voice and video over the network and hot-desking in the campus. Besides, the students can now have their E-learning that provides facilities such as real-time video and multimedia lectures.

2.5.2 Harvard Medical School

Harvard Medical School (HMS) includes 50 academic departments that employ approximately 13,000 full and part-time instructors, professors, researchers, residents, interns and post-doctoral fellows as well as 700 medical students. It has a large WLAN infrastructure with a wide variety of networking equipment is in use such as Nortel and Cisco switches, Cisco Access Points for 802.11b networks, Bluesocket Wireless LAN Gateways (for user authentication), and a multitude of wireless access cards and mobile devices. HMS employs 53 people in its central Information Technology Department to keep its computing systems and networks up and running.

This wireless initiative derived its guidelines and objectives from a meeting held by Harvard's University Technology Architecture Group (UTAG) in May 2002. The UTAG agreed to work towards a technical solution that is browser-based, supports SSL for encryption/security, and supports multiple authentication mechanisms that are Harvard University ID/PIN and standard end-user menu driven interface.

Based on the UTAG "Core Principles", HMS IT's Wish List, and an intensive evaluation process including trials in a non-production network, Harvard Medical School selected a solution based on Bluesocket Wireless LAN Gateways to support wireless networks throughout the campus.

Today, using Bluesocket's Wireless LAN Gateway products, wireless networks on the HMS campus are inter-connected in a way that simplifies wireless network management and improves the end-user experience while ensuring appropriate security, support for standards, and interoperability. Widespread wireless access is now possible from various locations around the HMS campus centered on the "HMS Wireless Quad." (See Appendix: Figure A-1).

When members of the HMS community attempt to log-on wirelessly, they are directed to a browser-based user interface that prompts them to select an authentication server, and then enter a user name and password combination. Bluesocket Wireless LAN Gateways then authenticate each user to HMS's LDAP directory maintained by HMS IT. Once authenticated, network users are then able to access network resources for which they have been authorized.

The HMS IT department recommends that wireless users of the HMS Wireless Quad use encryption techniques such as Secure Socket Layer (SSL), Virtual Private Networking (VPN), and Secure Shell (SSH) to protect from attacks and ensure the integrity and security of data transmissions. By channeling all wireless data traffic from wireless devices and access points through Bluesocket Wireless WLAN Gateways before it reaches the wired network, HMS-IT is able to run each user session in a separate IPsec tunnel and set appropriate levels of security to protect network resources and data transmissions from unwanted security breaches.

Each room in student housing is equipped with a 100MB connection, implemented with a certified CAT5e Ortronics cabling system and Nortel Baystack 450 fast Ethernet switches. Bluesocket's wireless gateway solutions give Harvard the infrastructure required to provide a standards-based, secure and 'seamless' user wireless experience across campus while still allowing 'local' management of wireless networks.

The benefits that they get by implementing wireless network in the campus includes MyCourses E-Curriculum that was rolled out in August 2001 following a pilot program that lets the students track their calendars, lecture locations, breaking school news and announcement virtually while reducing the need to print out reams of daily agendas and course notes as it is available online. Beside this, the students are now able to communicate among each other easily and even relaxing as faculty, staff and students can sip a cappuccino in the Wireless Quad's Courtyard Café while responding to e-mail or surfing the web. They also had launched eCommons, a project that lets community members create their own personalized desktop, and access electronic resources including websites and libraries, databases and e-mail directories.

As addition, they found out that wireless network are flexible as student could access it from anywhere at anytime. It also gives them mobility in medicine as Bluesocket's support for Secure Mobility—the ability to stay seamlessly and securely connected as wireless users move across subnets is a capability that our mobile students (in particular) have been asking for. It improves research done by their students because with wireless access availability at HMS's Countway Library of Medicine, students can use their laptop while conducting research at one of the great medical libraries to look up a resource, go to the resource online while in the stacks, find it, evaluate it and then place it into a bibliography or literature search database much more efficiently than in the days before wireless. Lastly, implementation of wireless networks maximizes limited physical space. Limiting the need to run networking cable through the walls and ceilings of facilities also reduces disruption, complications, support costs and repair visits.

2.5.3 Toyohashi University of Technology

Planex Communications Inc. had received an inquiry to purchase Planex's GW-AP110 Access Point from the network administrator of Toyohashi University of Technology. The network administrator had asked Planex for the AP capability of performing and relying three-way wireless communication that will be implemented in the university. As to fulfill the university needs, Planex had come out with a proposal for the implementation of GW-AP110 that could support inter-access point wireless communication. The reasons for the proposal are as follows:

- Three-way wireless communication is needed.
- The three LANs are not as far away from each other as to require inter-building wireless communication.
- The cost of implementing inter-building wireless communication (which includes costs of access points, antennae and installation expenses) can be quite high. On the other hand, the proposed plan can be implemented with minimum cost; GW-AP110 x 3 units: 33,000 yen x 3 (USD 254.10 x 3).

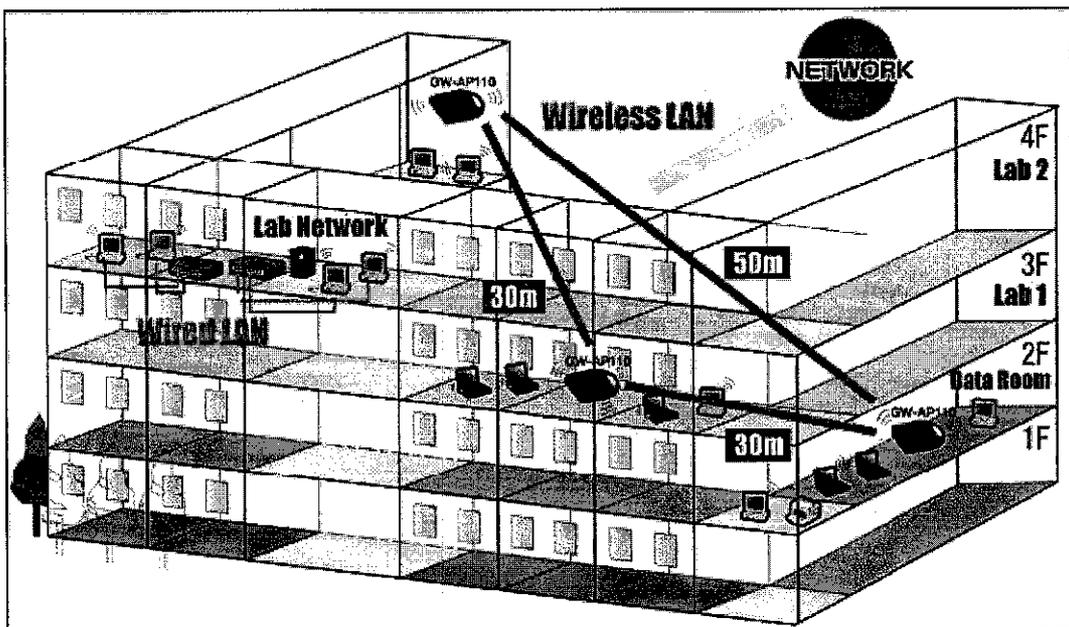


Figure 2.5: GW-AP110 placement in the building as proposed by Planex Communication Inc.

Figure 2.5 shows that there are three sites, which are Lab 1, Lab 2 and Data room that are connected via wireless LAN. One GW-AP110 access point is installed at each site, and the Lab Network is linked to the higher level university LAN. The node-to-node distances are as follows:

- Lab 1 (3F) - Lab 2 (4F): Approximately 30“m
- Lab 2 (4F) - Data Room (2F): Approximately 50“m
- Data Room (2F) - Lab 1 (3F): Approximately 30“m

The benefits that they get by integrating the network using access point includes manageable network, easy access from other floors and cost effective as they could save cost by manage it once rather than separately.

By referring to these case studies, a combination of incremented and different method techniques will be use to implement the project in UTP environment. For UTP, an access to up to 8000 users UTP-wide, with limited access in UTP area only, need to be considered. A different hardware and software will be used for WLAN in UTP. The details of the hardware and software will be discussed later, as this project proceeds.

CHAPTER 3

METHODOLOGY

3.1 PROCEDURE IDENTIFICATION

This methodology will take a combination and variation of the existing methodologies and apply it to suit the time frame condition and the huge amount of research needed. Figure 3.1 shows the methodology that is used in the development of this project, name as Custom Methodology.

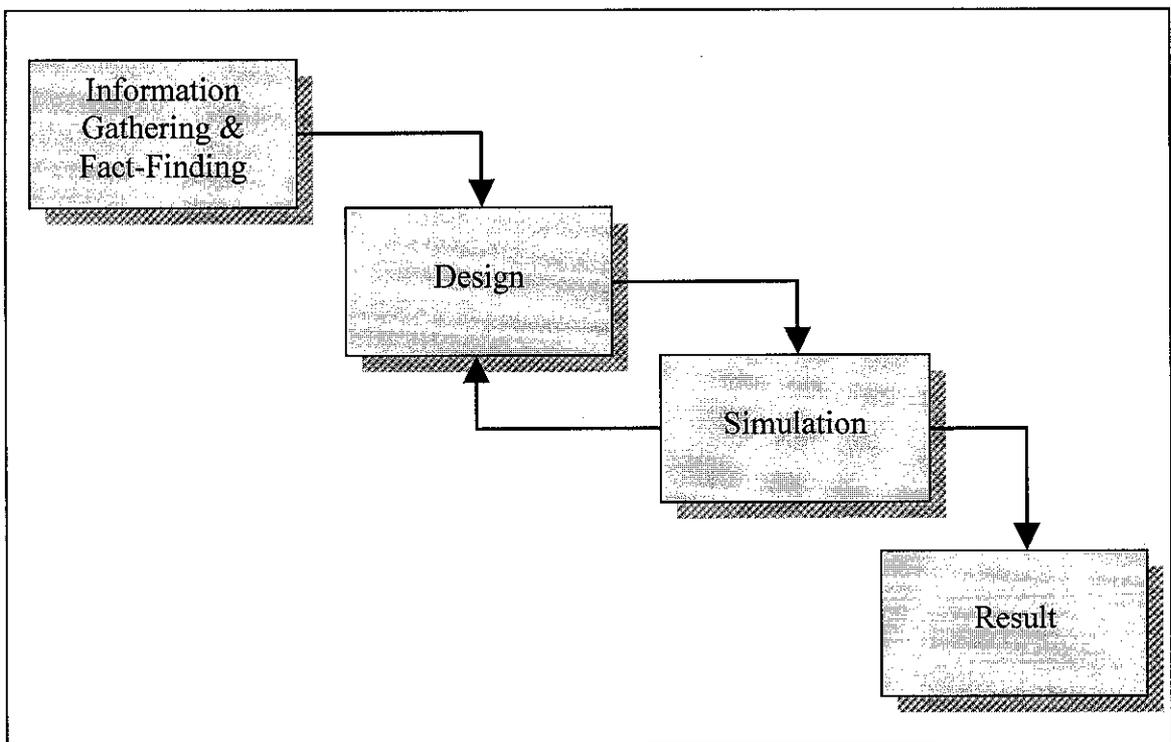


Figure 3.1: Custom Methodology used in this Project

3.1.1 Information Gathering and Fact-Finding

From Figure 3.1, there are four phases to complete this project. The first phase of this methodology will be information gathering and facts finding that involve research of previous project regarding the same area and fact-finding of WLAN. Before getting too far with the project, understanding of possible requirements, such as needs of users and applications, interfaces with existing systems, facility composition, and so on is important in this phase. This provides the basis for making decisions when designing the solution so it will meet user needs. Sources such as textbooks, telecommunication and wireless magazines, articles and journals are used as resource of information. A preliminary and feasibility study on potential hardware, software and concept that will be used in this project is done during this phase. This phase will took more than two months, as lots of research and survey need to be done before going to the next phase, which is the designing phase.

3.1.2 Design

After all the information is gathered and researches have been done, the design phase will take place. This phase will take approximately one month. The design produces a definition of how the wireless LAN will satisfy requirements. This includes technical elements such as developing the system architecture, identifying standards (e.g., 802.11b or 802.11a), selecting an access point vendor, specifying antennas types, identifying MAC Layer settings, and so on. The end result of the design will be a bill of materials and diagrams that indicate the interconnection of related software and hardware components. Of course this leads to the cost of the system, something important to know before moving on. In this phase, a proper arrangement of hardware such as AP and laptops is properly designed and arranged to get best network signal and performance. Plans will be drawn to help in recognize the placement of devices and its geographical factor.

3.1.3 Simulation

Upon the completion of the design process, a network simulation is done using network simulator existed in the market. This is done during simulation phase that will take less than a month. For this project, Network Simulator (NS) – Version 2 is used. NS is an event driven network simulator developed at UC Berkeley that simulates variety of IP networks. It implements network protocols such as TCP and UDP, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and more. NS also implements multicasting and some of the MAC layer protocols for LAN simulations. (Chung and Claypool, 2000)

The purpose of the simulation is to test and view the effectiveness of the network that was designed in previous phase. The simulator will shows how the wireless network signal is being distributed around its area and how strong and far it would be. To ensure this simulation works on Windows platform, a few guidelines need to be followed to get the NS-2 network simulator package to fully build on Cygwin environment for Microsoft Windows 9x/ME/NT/2000/XP. The major differences with the native Win32 build are to build all the components needed in one file, and the build process doesn't require VisualStudio to compile any component. Next, NAM would not run as a standalone Windows application, but within the Cygwin XFree86 server and a validation tests should be done in order to ensure the program works properly. At the beginning of a wireless simulation, the types for each of network components such as Link Layer (LL), Interface Queue (IfQ), MAC layer, and the wireless channel nodes transmit and receive signals from need to be defined. Additionally, other parameters like the type of antenna, the radio-propagation model, the type of ad-hoc routing protocol used by MobileNodes, and the number of maximum packet in IfQ are also need to be defined. The details of network components and parameters are described in Chapter 4. This process will refer back to the design phase, should any error occur in this phase.

3.1.4 Result

This project will end when results have been achieved. This is the fourth phase of this project. Results will contains all the come out from this project including the network

design for UTP, hardware and wireless tools specifications, and suggested wireless standard that should be used.

3.2 TOOLS REQUIRED

Some of the tools and hardware that has been identified for this project are as follows:

- A PC with Windows 2000 platform and above for both server and client.
- Network Simulator version 2 (ns-2) using Cygwin for Windows platform.
- An access point (AP).

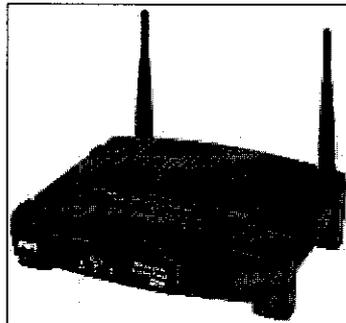


Figure 3.2: Example of an access point (AP)

- An 802.11a/b/g network card.
 - For laptop, this card will be normally a PCMCIA card that can be slide into the PCMCIA slot of the laptop, or a small external adapter that is plug into a USB port.

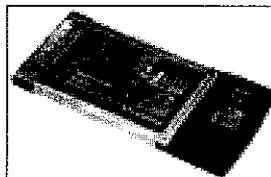


Figure 3.3: Example of PCMCIA wireless network card

- For desktop machine, a PCI card is installed inside the machine or a small external adapter that is connected to the computer with a USB cable.

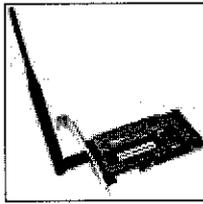


Figure 3.4: Example of PCI wireless network card

- Application software and that will connect user to the network.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Findings

4.1.1 General Findings

A few matters had been found throughout this project such as the hardware that is suitable to be used to implement wireless network, amount of access point needed and its placement in order to ensure the efficiency of the network, and the wireless standard that is suitable to be used in UTP environment. From the research that has been done, the minimum hardware requirement to implement wireless network is a server with Windows Server 2000 platform, an access point, an 802.11a/b/g network card, and a client PC with Windows 2000 platform and above. The AP placement should be not too far or too close to each other, and far from any obstacle such as walls and glasses. Adjustment of number and placement of clients could be done based on the equipment selected and its configuration. Physical and geographical factor is also the main concern regarding the amount and placement of AP. Lastly, the IEEE standard that is suitable to be used in UTP is 802.11g as it offers the same 54 Mbps of throughput like 802.11a do, which is useful for applications such as voice over WLAN and mobile videoconferencing. It operates in the 2.4 GHz band and was designed to be backwards compatible with 802.11b, which is suitable for checking e-mail and accessing presentations, documents, and the Web. 802.11g is the best standard to be used as these applications are most applied by UTP students.

4.1.2 Existing UTP Network Architecture

Figure 4.1 shows the UTP current network diagram. Basically, all UTP buildings are connected to IT Data Center at the Chancellor Complex via fiber optic cable. The

Chancellor Hall, Academic Blocks and Library are using multi-mode fiber optic cable with 8 cores as these buildings are closed to the IT Data Center. While the Villages, Village 1 to Village 5, are connected using single-mode fiber optic cable as they are far from the IT Data Center, i.e. more than two kilometers.

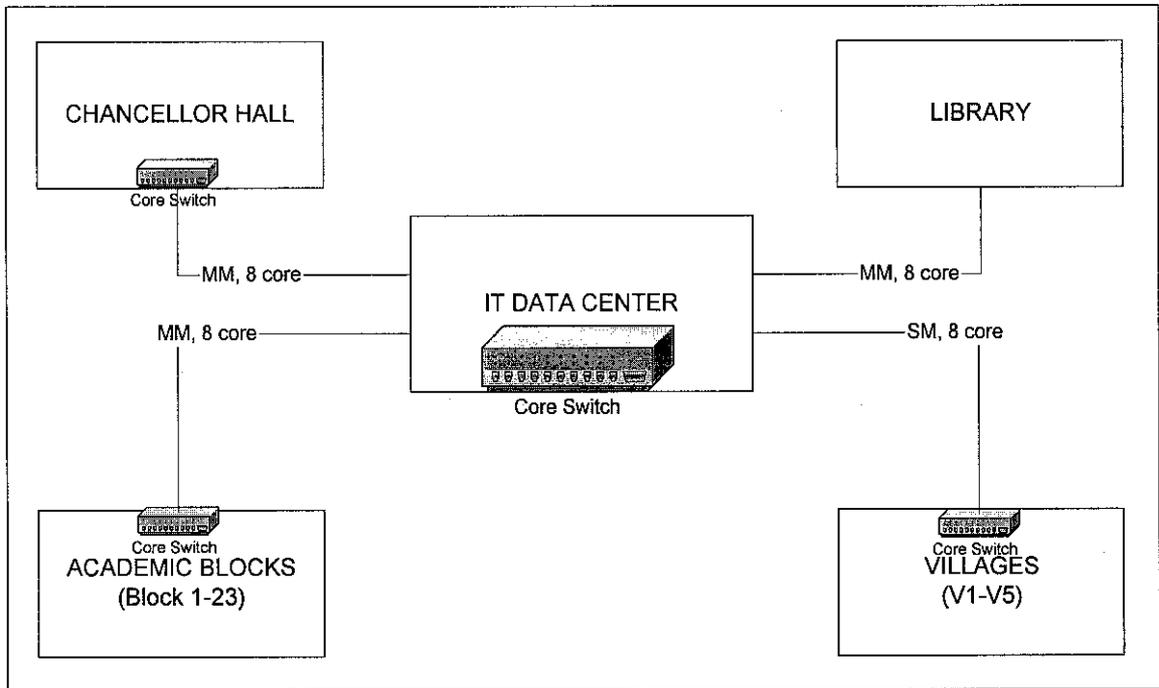


Figure 4.1: UTP Current Network Diagram

Figure 4.2 shows the new library network diagram, where there are four TCR (control room) on the first and second floor of the library. All workstations in the library are connected to the switches in the TCR rooms via wired network cable. These networks are connected directly from each TCR room to the IT Data Center, which is located at the Chancellor Complex basement. By using multi-mode fiber optic cable, the TCR rooms are directed to the core switch in the data center.

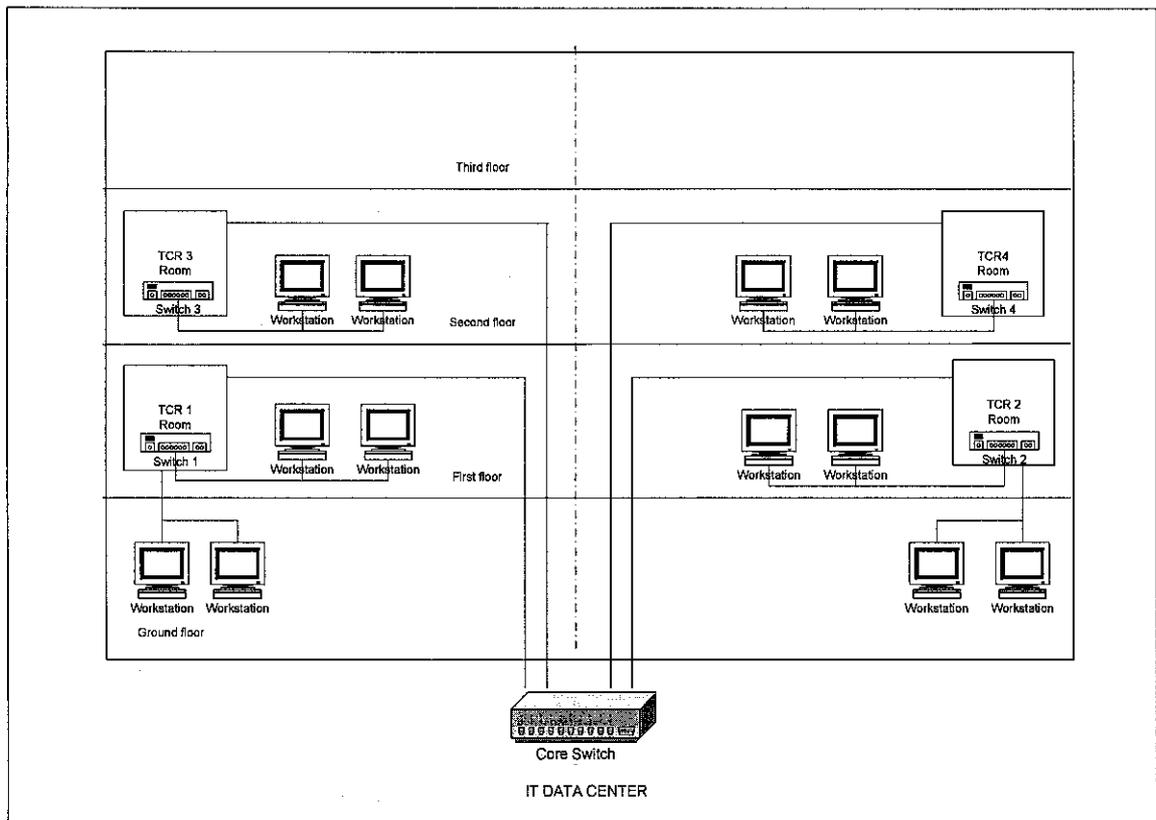


Figure 4.2: Library Current Network Diagram

Shown in the figures below are the architecture of Building 1 and 2 of Academic Complex for their respective floors. There are two server rooms at each block, which are located at first and second floor. Figure 4.3 shows the Building 1 and 2 ground floor layout. There are six application laboratories, two technician rooms, two utility rooms, two plant rooms and two telecommunication control rooms on the floor. Each laboratory contains approximately 30 workstations and each technician room has one desktop computer. These workstations and PC are connected to the switches which are located in the server room at first floor of each building.

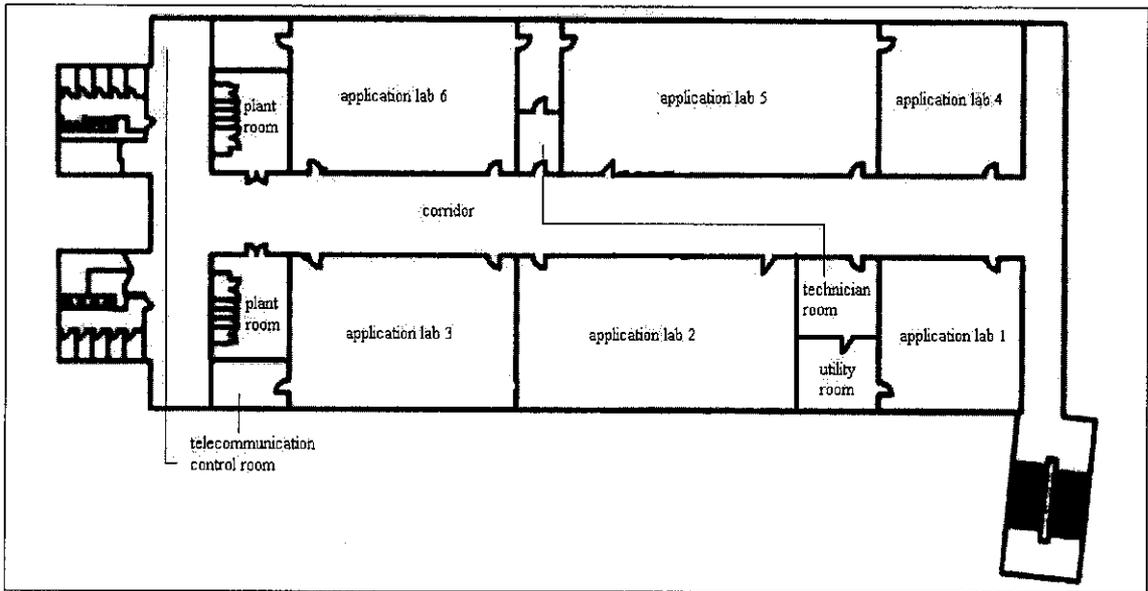


Figure 4.3: Building 1 and 2 ground floor layout

Next is the first floor and second floor architecture. There are also six laboratories on each floor. Each of the laboratories contains approximately 30 workstations. These workstations are connected to the server room. All workstations on the ground floor and first floor are connected to the server room that is located on the first floor. While all workstation on the second and third floor are connected to the server room, which is on the second floor. These are shown in Figure 4.4 and Figure 4.5 below.

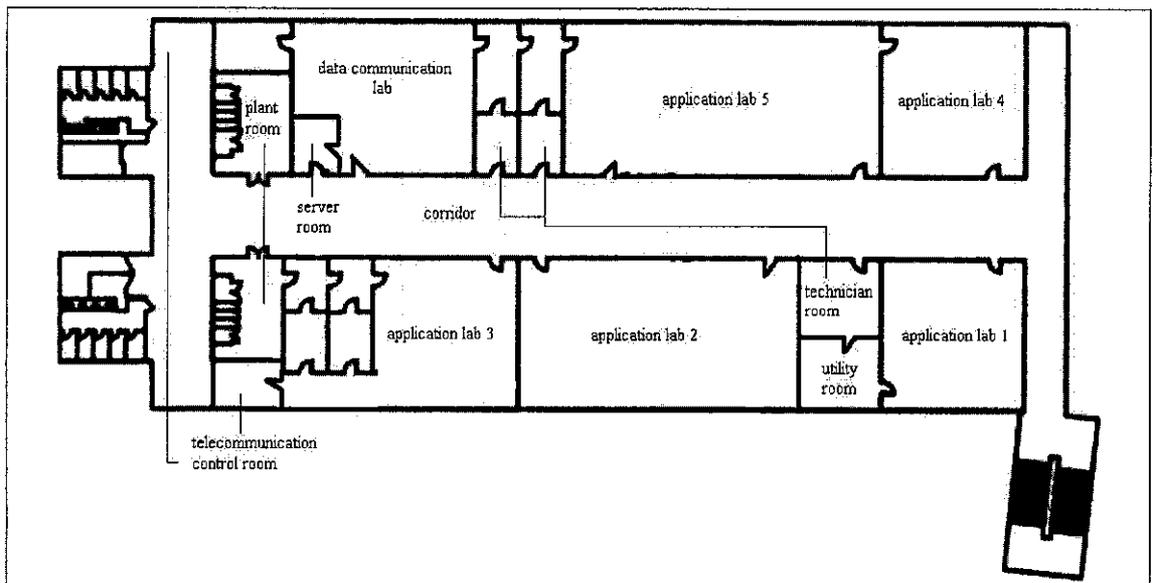


Figure 4.4: Building 1 and 2 first floor layout

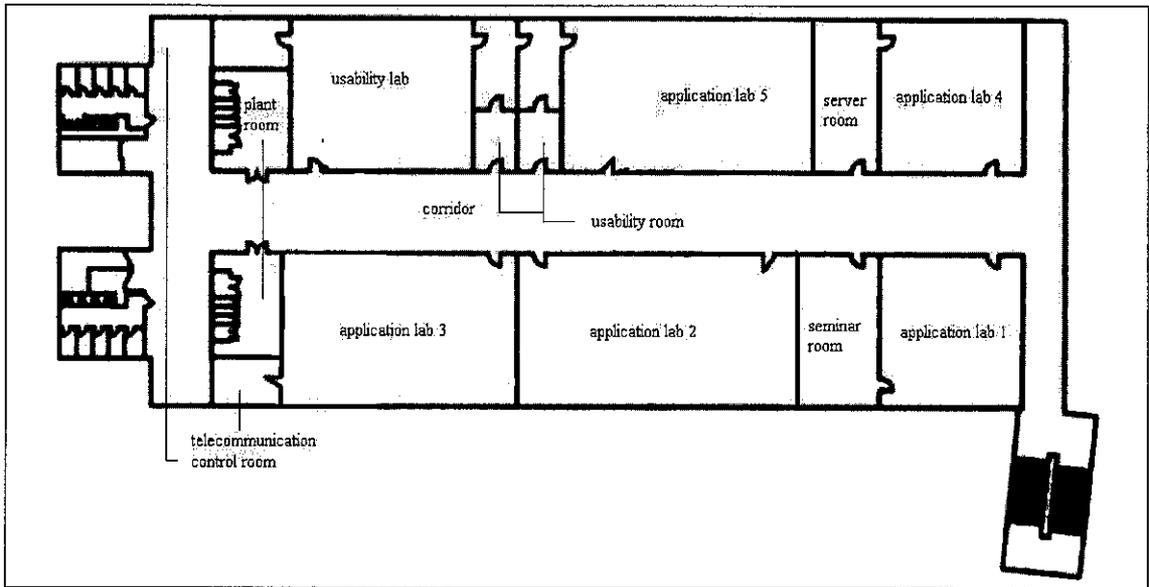


Figure 4.5: Building 1 and 2 second floor layout

The third floor of each building consists of lecturer's and tutor's rooms. There are 40 rooms including two meeting rooms and a utility room. The layout of the third floor is shown in Figure 4.6 below.

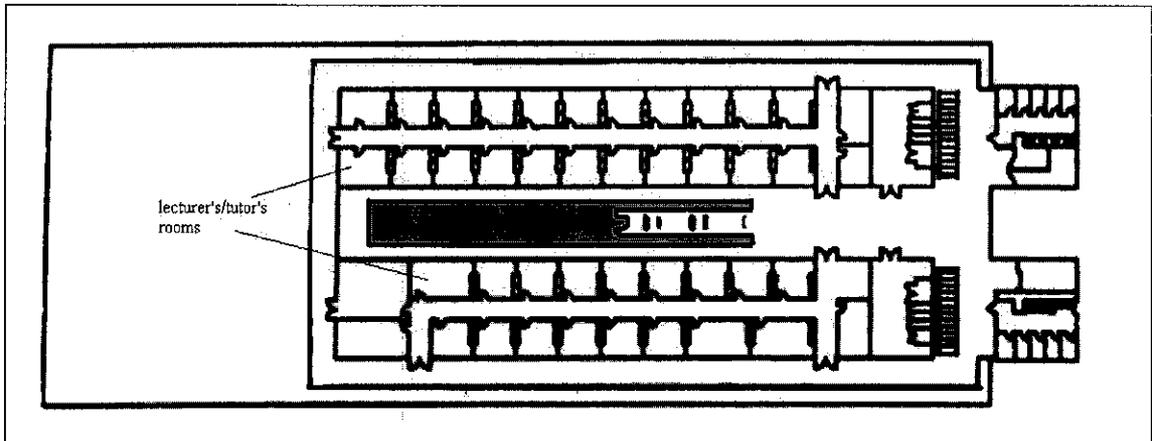


Figure 4.6: Building 1 and 2 third floor layout

4.1.3 Proposed UTP Network Architecture

From this architecture, a wireless network could be implementing by adding a 100 mbps Access Point (AP) to the existing port in the library. Figure 4.7 shows the proposed wireless network design for UTP's library. This design has yet not been tested. The AP could support up to 10 users at a time with range not more than 100 meters. The library

area, which is mostly covered by glasses needs more AP as the walls could limit the network bandwidth, thus will slow down the connection.

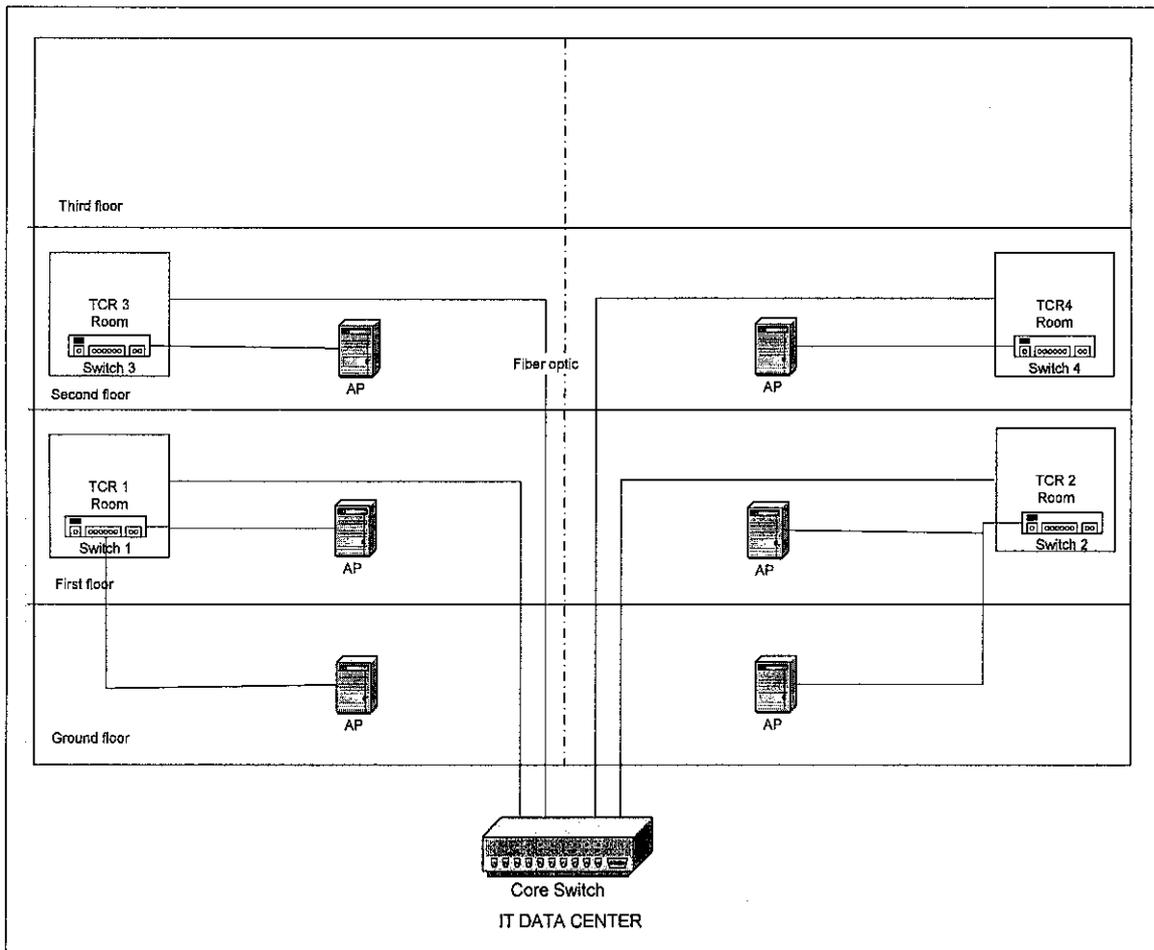


Figure 4.7: Proposed Wireless Network at Library

From this diagram, six APs are used, where two APs will be placed on each floor. These APs are placed on each side of respective floors. As library has wide spaces on every floor, less AP is needed. Each floor has their own IT zone where ports are available. AP could be connected to any of these ports as long as it could provide optimum bandwidth to the user. This architecture has not yet been tested. A test using network simulator, NS – Version 2, will be done after the network design is completed.

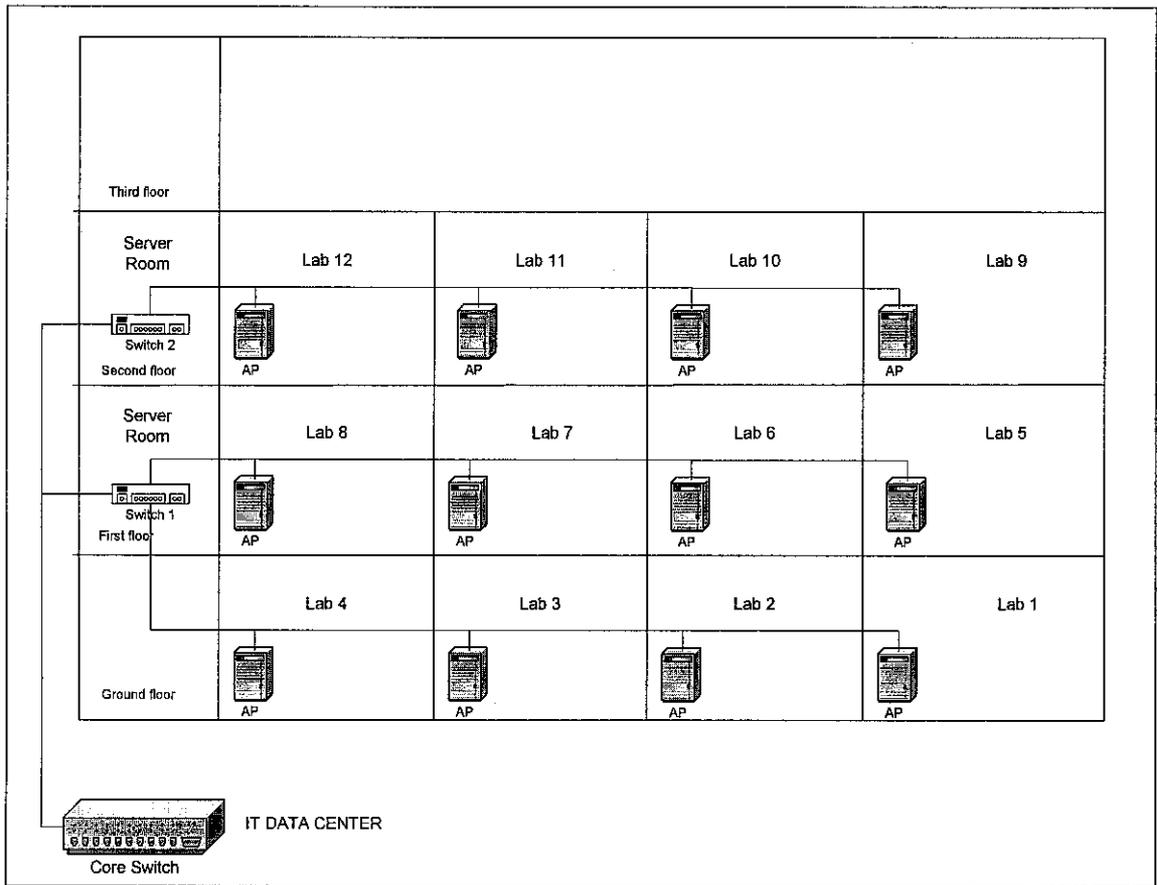


Figure 4.8: Proposed Wireless Network at Building 1 and 2 of Academic Complex

Figure 4.8 shows that the architecture of Building 1 and 2 in the Academic Complex is similar at every floor except third floor. An AP is needed in every lab as walls will block the signal and the connection cannot be access from outside the lab. These APs will be connected to the Server Room before the data is sent to IT Data Center via fiber optic cable. The lecturers' rooms, which are located on the third floor, are not provided with AP as every room has one port that will connect them directly to the server. This is also for security purpose as wireless network can easily be hacked by anyone at anytime. This could avoid incident such as stealing the exam question by the student from happened.

Finally is the wireless hardware setup diagram that can be implement in each of the laboratory rooms at Building 1 and 2.

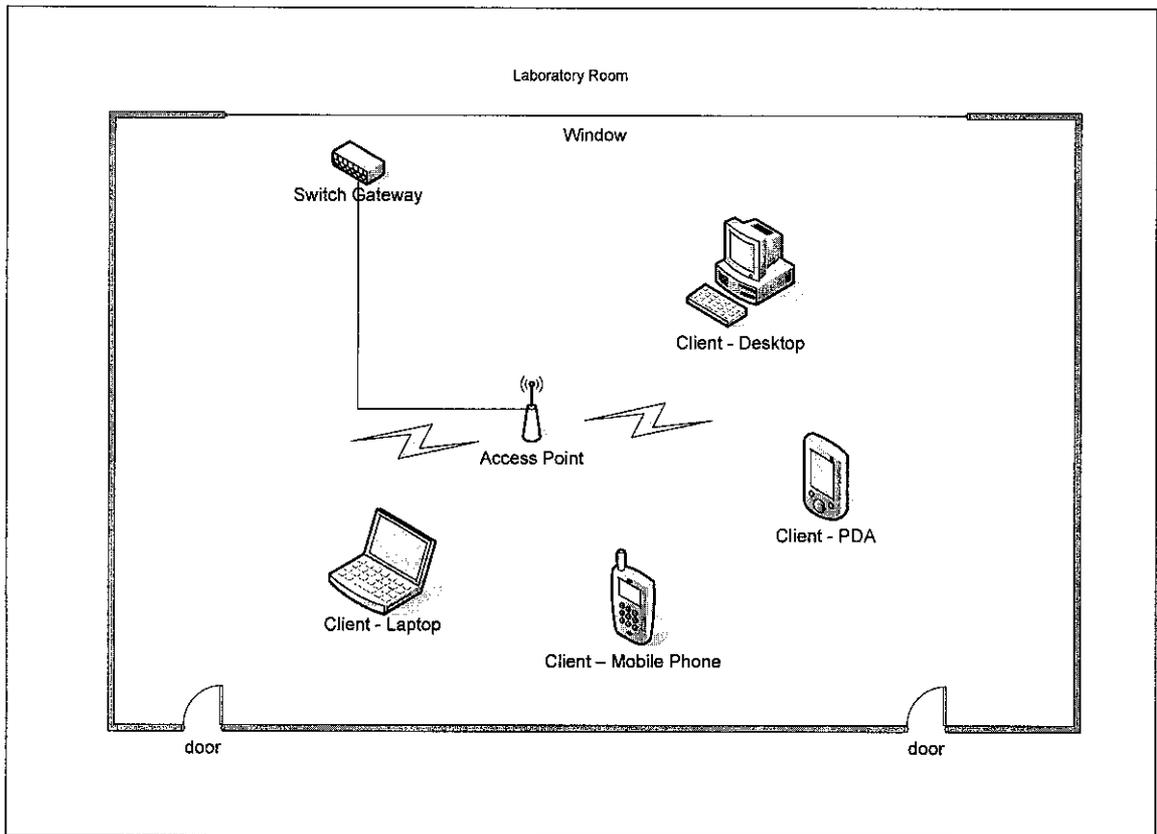


Figure 4.9: Wireless Hardware Setup Diagram

From the simulation result, a wireless network could be implemented as shown in Figure 4.9 above. Figure 4.9 shows that an access point is being access by multiple clients using multiple types of devices at one time. The access point is connected to a switch gateway that is located in the room. This switch is connected to a main switch in a server room located at second floor and third floor of the building (as shown in Figure 4.1). They are then directly being sent to the core switch at IT Data Center.

4.1.4 Simulation Result

Basically, the flow of NS-2 is shown in Figure 4.10 below. NS is Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries, and network setup (plumbing) module libraries (actually, plumbing modules are implemented as member functions of the base simulator object). Another major component of NS beside network objects is the event scheduler. An event in NS is a packet ID that is unique for a packet with scheduled time and the pointer to an

object that handles the event, where the scheduler will keep track of simulation time and fires all the events in the event queue scheduled for the current time by invoking appropriate network components.

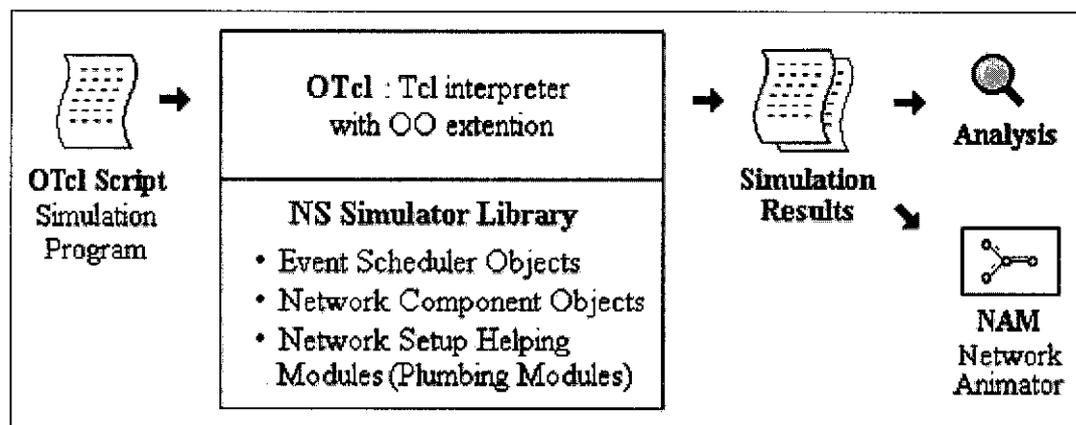


Figure 4.10: Simplified User's View of NS

When a simulation is finished, NS produces one or more text-based output files that contain detailed simulation data, if specified to do so in the input Tcl (or more specifically, OTcl) script. The data can be used for simulation analysis (two simulation result analysis examples are presented in later sections) or as an input to a graphical simulation display tool called Network Animator (NAM) that has a nice graphical user interface similar to that of a CD player (play, fast forward, rewind, pause and so on), and also has a display speed controller. Furthermore, it can graphically present information such as throughput and number of packet drops at each link, although the graphical information cannot be used for accurate simulation analysis. The exact simulation for UTP network design is still under testing, and the result will be reported in next report.

For this project, a simple wireless scenario in a lab is set up to test the simulation. The topology consists of eight nodes, which is node_(0) as the access point, node_(1), node_(2) , node_(5) and node_(6) indicates the mobilenodes, and node_(3), node_(4) and node_(7) as static nodes. See comments in the code below for a brief description of each variable defined.

1. Define variables that will be used in the simulation. The array used to define these variables, val() is not global.

```
# =====
# Define options
# =====
set val(chan)          Channel/WirelessChannel    ;# Channel Type
set val(prop)          Propagation/TwoRayGround   ;# radio-propagation model
set val(netif)         Phy/WirelessPhy           ;# network interface type
set val(mac)           Mac/802_11                ;# MAC type
set val(ifq)           Queue/DropTail/PriQueue    ;# interface queue type
set val(ll)            LL                        ;# link layer type
set val(ant)           Antenna/OmniAntenna       ;# antenna model
set val(ifqlen)        50                        ;# max packet in ifq
set val(nn)            8                         ;# number of mobilenodes
set val(rp)            DSDV                      ;# routing protocol
set val(x)             200
set val(y)             100
```

The parameters that had been defined are as follows:

Parameter	Value
Channel type	Wireless channel
Radio-propagation model	Two ray ground
Network interface type	Wireless physical
MAC type	802.11 standard
Interface queue type	Drop tail / PriQueue
Link layer type	LL (Link Layer)
Antenna model	Omni directional Antenna
Maximum packet used	50
Number of mobilenodes used	8
Routing protocol	DSDV
Coordinate area (x,y)	(200,100)

Table 4.1: Parameters defined in the simulation

2. We go to the main part of the program and start by creating an instance of the simulator,

```
set ns_ [new Simulator]
```

3. Setup traces and nam objects support by opening file wlan-out.tr and call the procedure trace-all {} as follows:

```
set tracefd [open mobile_network.tr w]
set namtrace [open mobile_network.nam w]
$ns_ trace-all $tracefd
$ns_ namtrace-all-wireless $namtrace $val(x) $val(y)
```

4. Create a topology object that keeps track of movements of mobilenodes within the topological boundary.

```
set topo [new Topography]
```

5. Load the topology values that had been defined before. We had earlier mentioned that mobilenodes move within a topology of 20m x 10m. But in this simulation, I had scale up the size to 10 times larger than the original size. We provide the topography object with x and y co-ordinates of the boundary, (x = 200, y = 100):

```
$topo load_flatgrid $val(x) $val(y)
```

The topography is broken up into grids and the default value of grid resolution is 1. A diferent value can be passed as a third parameter to load_flatgrid {} above.

6. We create the object God, as follows:

```
create-god $val(nn)
```

Quoted from CMU document on god, "God (General Operations Director) is the object that is used to store global information about the state of the environment, network or nodes that an omniscient observer would have, but that should not be made known to any participant in the simulation."

7. Create channel for each nodes.

```
set chan_1_ [new $val(chan)]
set chan_2_ [new $val(chan)]
set chan_3_ [new $val(chan)]
set chan_4_ [new $val(chan)]
set chan_5_ [new $val(chan)]
set chan_6_ [new $val(chan)]
set chan_7_ [new $val(chan)]
set chan_8_ [new $val(chan)]
```

8. Create mobilenodes. The node creation APIs has been revised and here we shall be using the new APIs to create mobilenodes. First, we need to configure nodes before we can create them. Node configuration API may consist of defining the type of addressing (flat/hierarchical etc), the type of adhoc routing protocol, Link Layer, MAC layer, IfQ etc. The configuration API can be defined as follows:

```
$ns_ node-config -adhocRouting $val(rp) \
                -llType $val(ll) \
                -macType $val(mac) \
                -ifqType $val(ifq) \
```

```

-ifqLen $val(ifqlen) \
-antType $val(ant) \
-propType $val(prop) \
-phyType $val(netif) \
-topoInstance $topo \
-agentTrace ON \
-routerTrace ON \
-macTrace ON \
-movementTrace OFF \
-channel $chan_1_

```

The above procedure creates a mobilenode (split) object, creates an adhoc-routing routing agent as specified, creates the network stack consisting of a link layer, interface queue, MAC layer, and a network interface with an antenna, uses the defined propagation model, interconnects these components and connects the stack to the channel.

9. Create nodes as follows:

```

set node_(0) [$ns_ node]
set node_(1) [$ns_ node]
set node_(2) [$ns_ node]
set node_(3) [$ns_ node]
set node_(4) [$ns_ node]
set node_(5) [$ns_ node]
set node_(6) [$ns_ node]
set node_(7) [$ns_ node]

#disable random motion for all nodes

$node_(0) random-motion 0
$node_(1) random-motion 0
$node_(2) random-motion 0
$node_(3) random-motion 0
$node_(4) random-motion 0
$node_(5) random-motion 0
$node_(6) random-motion 0
$node_(7) random-motion 0

```

10. Add the following lines for providing initial position of nodes in nam. However, note that only node movement can currently be seen in nam. 20 defines the node size in nam, must adjust it according to the scenario size; for this simulation the scenario size is scale up to 10 times larger than the actual size. The function must be called after mobility model is defined.

```

for {set i 0} {$i < $val(nn)} {incr i} {
    $ns_ initial_node_pos $node_($i) 20
}

```

11. Give the nodes a position to start with,

```

# Provide initial (X,Y, for now Z=0) co-ordinates for mobilenodes

$node_(0) set X_ 50.0

```

```

$node_(0) set Y_ 50.0
$node_(0) set Z_ 0.0

$node_(1) set X_ 0.0
$node_(1) set Y_ 0.0
$node_(1) set Z_ 0.0

$node_(2) set X_ 10.0
$node_(2) set Y_ 20.0
$node_(2) set Z_ 0.0

$node_(3) set X_ 1.0
$node_(3) set Y_ 1.0
$node_(3) set Z_ 0.0

$node_(4) set X_ 5.0
$node_(4) set Y_ 70.0
$node_(4) set Z_ 0.0

$node_(5) set X_ 50.0
$node_(5) set Y_ 70.0
$node_(5) set Z_ 0.0

$node_(6) set X_ 50.0
$node_(6) set Y_ 20.0
$node_(6) set Z_ 0.0

$node_(7) set X_ 130.0
$node_(7) set Y_ 97.0
$node_(7) set Z_ 0.0

```

The starts positions for the nodes are as follows:

Node number	Position (coordinate)
0	(50,50)
1	(0,0)
2	(10,20)
3	(1,1)
4	(5,70)
5	(50,70)
6	(50,20)
7	(130,97)

Table 4.2: Nodes start positions

12. Produce some node movements,

```

# Node_(1), node_(2), node_(5), and node_(6) starts to move towards node_(0)
# node_(3), node_(4), and node_(7) remains at their places

$ns_ at 0.0 "$node_(0) setdest 50.0 50.0 0.0"
$ns_ at 2.0 "$node_(1) setdest 25.0 14.0 5.0"
$ns_ at 3.0 "$node_(2) setdest 10.0 25.0 5.0"
$ns_ at 0.0 "$node_(3) setdest 1.0 1.0 5.0"
$ns_ at 0.0 "$node_(4) setdest 5.0 70.0 5.0"
$ns_ at 3.0 "$node_(5) setdest 30.0 90.0 5.0"
$ns_ at 0.0 "$node_(6) setdest 30.0 2.0 5.0"
$ns_ at 0.0 "$node_(7) setdest 130.0 97.0 0.0"

# Node_(1) then starts to move away from node_(0)
$ns_ at 5.0 "$node_(1) setdest 170.0 18.0 27.0"

# Node_(2) then starts to move away from node_(0)

```

```

$ns_ at 10.0 "$node_(2) setdest 190.0 95.0 70.0"

# Node_(5) then starts to move away from node_(0)
$ns_ at 13.0 "$node_(5) setdest 50.0 90.0 33.0"

# Node_(6) then starts to move away from node_(0)
$ns_ at 18.0 "$node_(6) setdest 60.0 1.0 87.0"

```

\$ns_ at 2.0 "\$node_(1) setdest 25.0 14.0 5.0" means at time 2.0s, node 1 starts to move towards the destination (x=25, y=14) at a speed of 5m/s. This API is used to change direction and speed of movement of the mobilenodes. The details of nodes movement are as follows:

Node	Time Start (s)	Destination (x,y)	Speed (m/s)
0	0.0	(50,50)	0.0
1	2.0	(25,14)	5.0
2	3.0	(10,25)	5.0
3	0.0	(1,1)	5.0
4	0.0	(5,70)	5.0
5	3.0	(30,90)	5.0
6	0.0	(30,2)	5.0
7	0.0	(130,97)	0.0

Table 4.3: Values defined for node movement

13. Setup traffic flow between the nodes as follows:

```

# TCP connections between node_(0) and node_(1)

set tcp [new Agent/TCP]
$tcp set class_2
set sink [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp
$ns_ attach-agent $node_(1) $sink
$ns_ connect $tcp $sink
set ftp [new Application/FTP]
$ftp attach-agent $tcp
$ns_ at 3.0 "$ftp start"

# TCP connections between node_(0) and node_(2)

set tcp2 [new Agent/TCP]
$tcp2 set class_2
set sink2 [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp2
$ns_ attach-agent $node_(2) $sink2
$ns_ connect $tcp2 $sink2
set ftp2 [new Application/FTP]
$ftp2 attach-agent $tcp2
$ns_ at 4.0 "$ftp2 start"

# TCP connections between node_(0) and node_(3)

set tcp3 [new Agent/TCP]
$tcp3 set class_2
set sink3 [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp3
$ns_ attach-agent $node_(3) $sink3

```

```

$ns_ connect $tcp3 $sink3
set ftp3 [new Application/FTP]
$ftp3 attach-agent $tcp3
$ns_ at 5.0 "$ftp3 start"

# TCP connections between node_(0) and node_(4)

set tcp4 [new Agent/TCP]
$tcp4 set class_ 2
set sink4 [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp4
$ns_ attach-agent $node_(4) $sink4
$ns_ connect $tcp4 $sink4
set ftp4 [new Application/FTP]
$ftp4 attach-agent $tcp4
$ns_ at 6.0 "$ftp4 start"

# TCP connections between node_(0) and node_(5)

set tcp5 [new Agent/TCP]
$tcp5 set class_ 2
set sink5 [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp5
$ns_ attach-agent $node_(5) $sink5
$ns_ connect $tcp5 $sink5
set ftp5 [new Application/FTP]
$ftp5 attach-agent $tcp5
$ns_ at 7.0 "$ftp5 start"

# TCP connections between node_(0) and node_(6)

set tcp6 [new Agent/TCP]
$tcp6 set class_ 2
set sink6 [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp6
$ns_ attach-agent $node_(6) $sink6
$ns_ connect $tcp6 $sink6
set ftp6 [new Application/FTP]
$ftp6 attach-agent $tcp6
$ns_ at 8.0 "$ftp6 start"

# TCP connections between node_(0) and node_(7)

set tcp7 [new Agent/TCP]
$tcp7 set class_ 2
set sink7 [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp7
$ns_ attach-agent $node_(7) $sink7
$ns_ connect $tcp7 $sink7
set ftp7 [new Application/FTP]
$ftp7 attach-agent $tcp7
$ns_ at 10.0 "$ftp7 start"

```

This sets up a TCP connection between the nodes with a TCP source on node 0. The packets start sending at time as shown in the table below:

Node	Time start (s)
1	3.0
2	4.0
3	5.0
4	6.0
5	7.0
6	8.0
7	10.0

Table 4.4: Start time of sending packet for each nodes

14. Define stop time when the simulation ends and tell mobilenodes to reset which actually resets their internal network components.

```

for {set i 0} {$i < $val(nn)} {incr i} {
    $ns_ at 25.0 "$node_($i) reset";
}
$ns_ at 25.0 "stop"
$ns_ at 25.01 "puts \"NS EXITING...\" ; $ns_ halt"
proc stop {} {
    global ns_ tracefd
    $ns_ flush-trace
    close $tracefd
}

```

At time defined, \$val (stop), the simulation shall stop. The nodes are reset at that time and the "\$ns_ halt" is called at 25.01s, a little later after resetting the nodes. The procedure stop {} is called to flush out traces and close the trace file.

15. Start the simulation,

```

puts "Starting Simulation..."
$ns_ run

```

The file is saved as "mobile_network_final.tcl". After running this file, we have to open the output file for this file, named mobile_network.nam to view the animator. Shown below in Figure 4.11 is the NAM environment. As we turned on the AgentTrace and RouterTrace, routing messages and packets are being received and sent by Router and Agent object in node 0 and node 1 until node 7. Shown in the simulation also is the wireless signal, which indicates the network is currently being access by nodes. Figure 4.11 shows that the nodes start to move at time 0.0s.

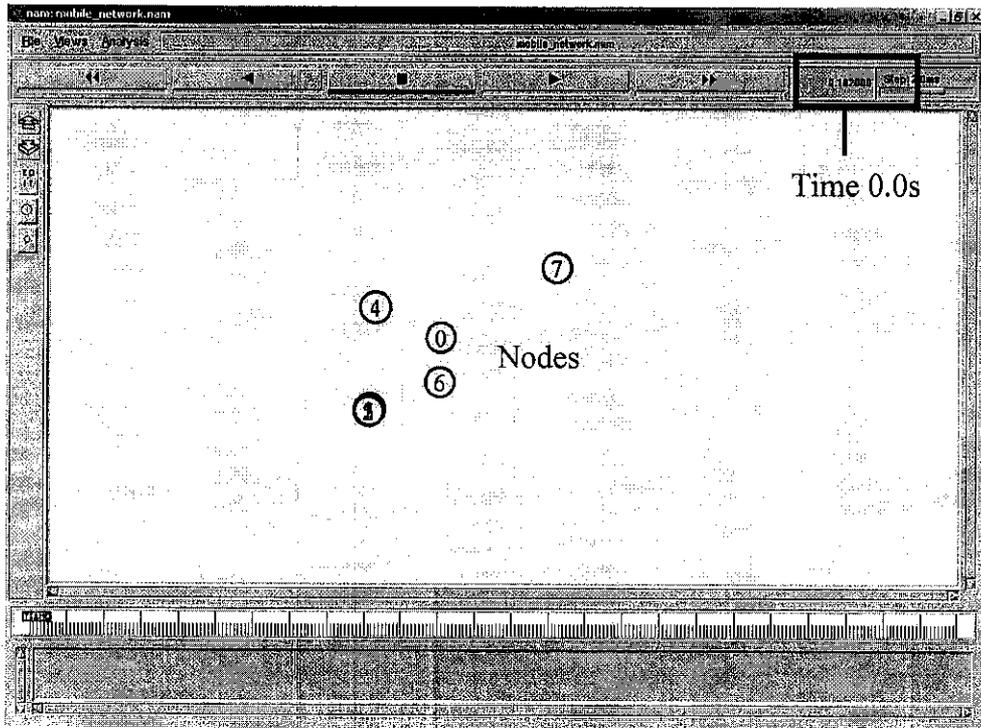


Figure 4.11: Nodes start to move to their destination at time 0.0s

At time 3.0s the routing info begins to be exchanged between both the nodes and AP, and the packet is being received by node 1 which then sends an ACK back to node 0 and the connection is setup. Same scenario is applied to the other nodes depending on their start time.

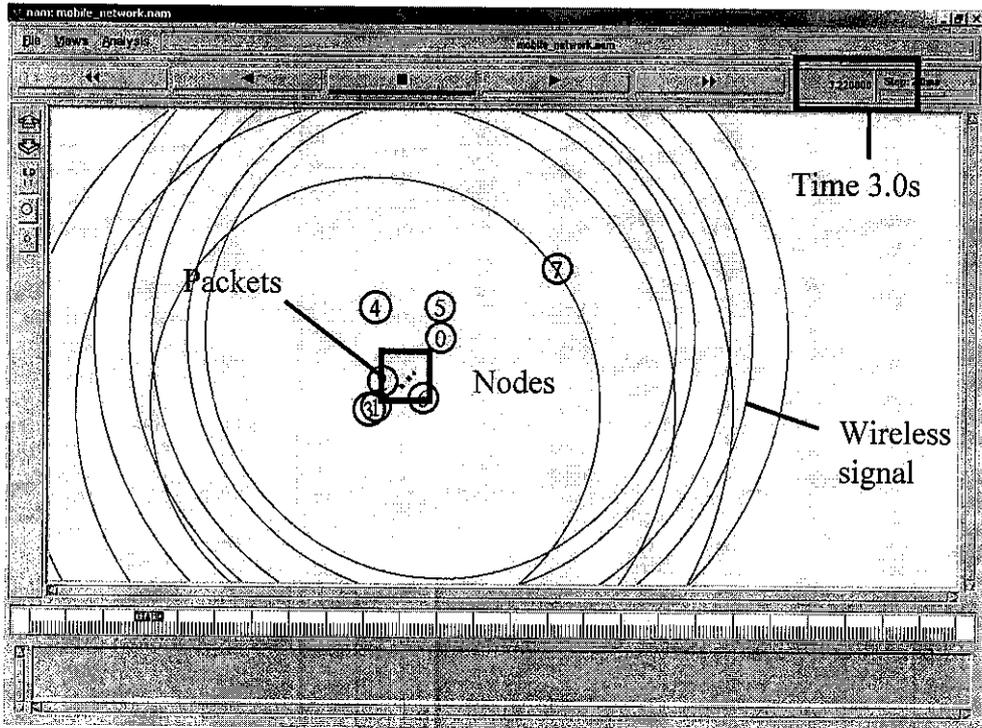


Figure 4.12: Wireless signal starts and node 1 start send packets at time 3.0s

Figure 4.12 show that node 1 is receiving a signal from the access point. This shows that the node is alive. The other nodes also showing the signal by interval time of 1.0 seconds. Finally, as node 1, node 2, node 5 and node 6 moves away from node 0, the packets started getting drop that happen at time 20.0s as shown in Figure 4.12 below. the remaining static nodes; node 3, node 4 and node 7 are still receiving and acknowledging packets with node 0 as they are not move and remain in the coverage area.

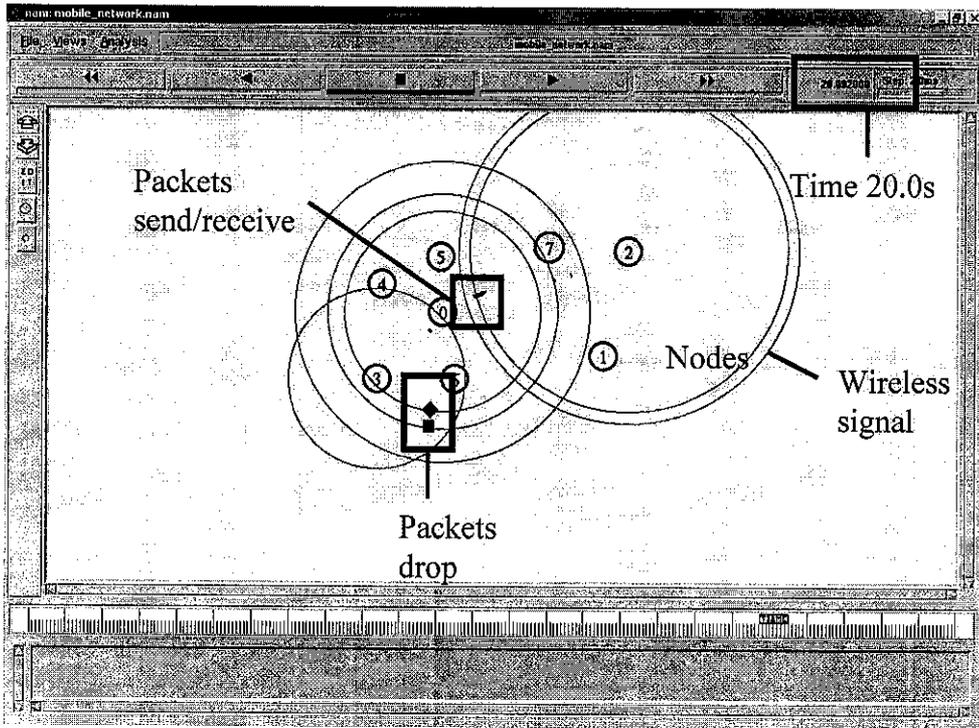


Figure 4.13: Packets drop as nodes move away

As the simulation reaching its stop time, 25.0s, the packets are dropping and connection between nodes are terminated. This is shown in Figure 4.14 below.

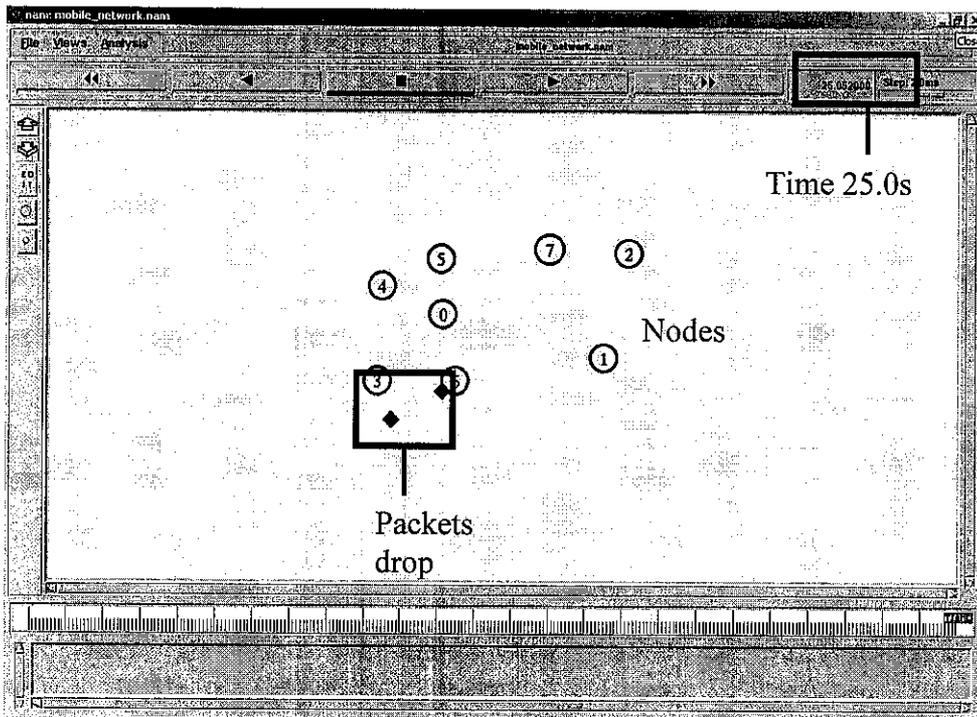


Figure 4.14: Packet drops after reaching stop time, 25.0s

4.1.5 Conclusion from the simulation

From the simulation result, it is found out that as the nodes start to move away from the AP, the packets will start dropping and the connection might be lost after it moves out from the coverage area. So, all nodes should be in the coverage area so that they could connect to the AP. As addition, when the number of nodes is added, the packets sent will also drop gradually as the AP needs to transfer the packets to other nodes too. More nodes require more bandwidth. An AP could support up to 20 clients at one time depending on its specification and standard.

4.2 Discussion

4.2.1 Wireless environment

There is much information that had been found upon completion of this report. It is said that wireless LAN (WLAN) could extend network to every square inch of buildings, campus or residence without the physical limitations of wires or cables so that a network connection could be established. WLAN can be an alternative opportunity for an organization to build a network connection instead of using the traditional wired LAN. It is an exciting technology that enables computer users to access file stored on a network while moving around or working in a temporary office space.

It is also found that finding the optimal locations for wireless equipment such as AP is important for its performance, and can be achieved by measuring the relative signal strength of the AP. All factors that could contribute to the low performance of wireless network such as distance, obstructions, or interference need to be clarified. There are some guidelines regarding the placement of wireless equipment found during the completion of this report that can be used for this project. Organizations are advised to install the AP at a central location as clients that are too far away from the base station will manage only 10% - 50% the bandwidth of clients nearby to it. Next, it is necessary to avoid physical obstructions whenever possible. Any barriers along the "line of sight" between client and base station will degrade a Wi-Fi radio signal. Plaster or brick walls are likely to have the most negative impact, but really any obstruction including cabinets or furniture will fail the signal to some degree.

Obstructions tend to reside closer to floor level. Therefore, many folks prefer to install their base station on or near the ceiling. Besides, Wi-Fi signals literally bounce off of windows, mirrors, or stainless steel countertops and other reflective surfaces that will result in lessening both network range and performance. Home appliances such as microwave ovens, cordless telephones, baby monitors, and home automation equipment like X-10 devices can generate interference as it transmits in the same general range as 802.11b or 802.11g (2.4 GHz). To avoid this, users need to install the AP at least one

meter away from other home appliances that send wireless signals in the same frequency range and Avoid electric fans, other motors, and fluorescent lighting.

Limitation of access for only inside UTP area is also a major concern as this project focus only in UTP environment. A combination of incremented and different method techniques from the case study found in this report will be use as a guideline to implement this project in UTP environment.

4.2.2 Simulation Results

The wireless model essentially consists of the MobileNode at the core, with additional supporting features that allows simulations of multi-hop ad-hoc networks, wireless LANs. As mentioned in previous chapter, a MobileNode consists of network components like Link Layer (LL), Interface Queue (IfQ), MAC layer, and the wireless channel nodes transmit and receive signals from. At the beginning of a wireless simulation, the types for each of these network components need to be defined. Additionally, other parameters like the type of antenna, the radio-propagation model, the type of ad-hoc routing protocol used by mobilenodes, and the number of maximum packets in IfQ are also need to be defined.

There are eight nodes used in this simulation, which node 0 was assigned as an access point, while the remaining seven nodes are clients. As the nodes start to move away from the AP, the packets will start dropping and the connection might lost after it moves out from the coverage area. From this result, it is found out that all nodes should be in the coverage area so that they could connect to the AP. As addition, when the number of nodes is added, the packets send will also drop gradually as the AP needs to transfer the packets to other nodes too.

CHAPTER 5

RECOMMENDATION AND CONCLUSION

5.1 Recommendation

Throughout the completion of this project, I have found out that this project could be continued by designing the wireless network architecture in more locations in UTP environment such as cafes, lecture halls, and lecture rooms, as this project limits to only implement it in academic building area only. More considerations and problems such as obstacles and physical environment need to be justified if implementation of wireless network is done at open area such as cafes. Furthermore, the network simulation tool used, which is Network Simulator Version 2 (NS-2), need to be studied more as it allows many types of network simulation and consume times to study it.

A simple network simulation tools that provides drag-and-drop function with built in components, could also be used to replace the ns. As for recommendation, student could use the OPNET Modeler as an alternative tool for network simulation. This is because; OPNET software (with model source code) is available for FREE to the academic research and teaching community (but need to be apply by the university), OPNET's discrete event engine for network simulations is the fastest and most scalable commercially available solution, it design the most precise and flexible simulations with over 400 documented API functions, and finally, OPNET provides automated model generation capability from live data, more detailed model libraries, and the most capable model development GUI in the industry (does not affect simulation runtime performance).

Lastly, a real hardware setup could also be implementing to show how the real stuff works in the real environment. This will show the outcome of the designed wireless

network architecture in more realistic manner. It also helps to approximate the maximum bandwidth of wireless signal and its limitations.

5.2 Conclusion

This project shows that wireless LAN (WLAN) could be used in UTP as alternative opportunities to convenient networking. This is because WLAN could extend network to every square inch of buildings, campus or residence without the physical limitations of wires or cables so that a network connection could be established. It is beneficial to UTP students and staff as it gives convenient network connection in campus environment. WLAN consists of access points (AP) and terminals that have WLAN connectivity and a network card is required in order to connect to the network.

There are a few factors that need to be considered before implementing the wireless network design such as geographical and physical area of the network and also its limitation and the suitable IEEE standard that will be used. The arrangement of the equipment such as AP needs to be properly done so that high performance of network connection could be obtained. In this project, six AP is proposed to be used in the library, and an AP is needed in every lab at every floor of Building 1 and 2. From the simulation, it is recommended that each laboratory rooms should have one AP that connected to a switch as shown in Figure 4.9. The placement of this hardware is also shown in Figure 4.9. As the simulation starts, the results shows that the routing messages and packets being received and sent. However, as the nodes start to move away from each other, connection breaks down occur, which cause the packets drop. This shows that all nodes should be within the coverage area to ensure that the network connection is strongly available.

The IEEE standard that will be used in UTP is 802.11g as it offers the same 54 Mbps of throughput like 802.11a do, which is useful for applications such as voice over WLAN and mobile videoconferencing. The main advantage of 802.11g over 802.11a is that it operates in the 2.4 GHz band and was designed to be backwards compatible with 802.11b, which is suitable for checking e-mail and accessing presentations, documents,

and the Web. 802.11g is the best standard to be used as these applications are most applied by UTP students. This project should come out with a proper wireless network design that could gives optimum performance by referring to the simulation result.

REFERENCES

1. How Stuff Works: *How Wi-Fi Works*, 2004.
<http://money.howstuffworks.com/wireless-network.htm>
2. Jamil Farshchi, October 14, 2003, “*Evaluating Wireless Networks*” in PCIE IT Roundtable Workshop, NASA.
<http://www.hq.nasa.gov/office/oig/hq/ITR/ITRpresentationwireless.ppt>
3. Bradley Mitchell, 2004, “*Your Guide to Wireless/Networking*”, article from CompNetworking. Available at <http://compnetworking.about.com>
4. Jim Barthold, 21st June 2004, *SUPERCOMM: Wireless Network to Converge*, Telecom Flash of Telecommunication™ Magazine.
<http://www.telecomflash.com>
5. ABC Data, a division of UNIKA from Germany.
<http://www.abcddata.de>
6. Asma Yasmin, 11th October 1999, *Known Vulnerabilities in Wireless LAN Security*, thesis, Helsinki University of Technology.
http://www.tml.hut.fi/Studies/Tik-110.300/1999/Wireless/vulnerability_4.html
7. Molta Dave, March 1999, Foster-Webster Areth, “*Wired on Wireless: A New Class of 802.11 Devices Go the Distance*”.
<http://www.networkcomputing.com/1006/1006r2.html>
8. Anthony Adshed, 27th May 2003, “*Building the Network of Your Dreams*” article from ComputerWeekly.com journal.
<http://www.computerweekly.co.uk/Article122007.htm>

9. Nortel Networks™, 2003, "*The Power of One Network – Securing and Scaling the Wireless LAN*", Position Paper available at <http://www.nortelnetworks.com>.
10. Bluesocket, Inc. 2002, "*Wireless at 'The Med School': Past, Present and Future*", Case Study: Planning and Operating a Wireless Authentication and Policy Management System at Harvard Medical School, journal from Bluesocket, Inc. Available at <http://www.hms.harvard.edu/it/wireless/index.html>.
11. Del Smith, January 2003, "*Get IT Done: How to place your wireless access point*" article from CNET Networks, Inc., available at <http://www.techrepublic.com>
12. Bradley Mitchell, 2004, "*How to Optimally Position a Wireless Access Point or Router*", article from CompNetworking, available at <http://compnetworking.about.com>
13. Richard Stone, 2004, "*5 Steps to Setting up a Wireless Network*", article from Entrepreneur.com.
14. Alex Hills, Jon Schlegel, and Ben Jenkins, January 2004, "*Estimating Signal Strengths in the Design of an Indoor Wireless Network*", journal: IEEE Transactions on Wireless Communications, Vol. 3, Issue 1. Available at <http://www.ieee.org/ieeexplore>
15. James Kaczman, September 2002, "*Wi-Fi Hotspot Networks Sprout like Mushrooms*", journal: IEEE Spectrum. Available at <http://www.ieee.org/ieeexplore>
16. Ajay Chandra V. Gummalla, *Student Member, IEEE*, and John O. Limb, *Fellow, IEEE*, September 2000, "*Design of an Access Mechanism for a High Speed Distributed Wireless LAN*", journal: IEEE Journal on Selected Areas in Communications, Vol. 18, Issue 9. Available at <http://www.ieee.org/ieeexplore>

17. Jae Chung and Mark Claypool, 2000, "*NS by Example*", project report for Worcester Polytechnic Institute. Available at <http://nile.wpi.edu/NS/FAQ.html>
18. Marc Greis, 2000, "*Tutorial for the Network Simulator "ns"*", a tutorial available in the ns package.
19. "Quick Guide For Hotspot Access: Windows XP version XP 2", user guide available at www.hotspot.ne.jp/en/pdf/hotspot_manual.pdf in pdf format.
20. Chris De Herrera, 2000, "*802.11 Wireless LAN Configuration*", online article from Windows CE Website. Available at <http://www.cewindows.net/>
21. UARK article, "*Getting Connected and Browsing the Web via Your Wireless PDA*", online article by UARK's Computer Service. Available at <http://www.uark.edu/compserv/softsys/pda/ipnexuspda.html>

APPENDICES

APPENDIX A

HARVARD MEDICAL SCHOOL (HMS) WIRELESS QUAD LOCATIONS

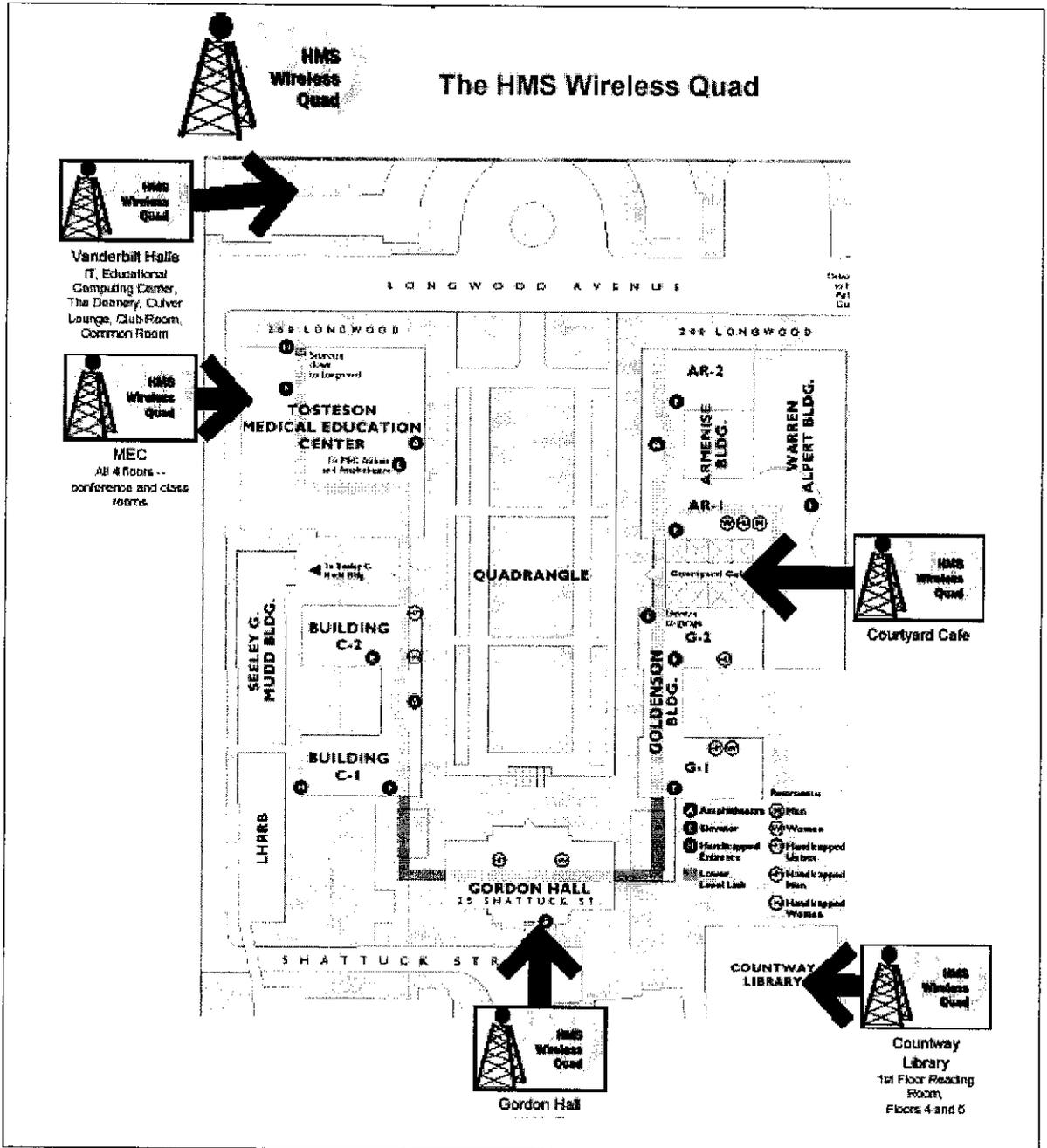


Figure A-1: The HMS Wireless Quad Locations

APPENDIX B

WIRELESS NETWORK DEVICES AND PRICES

List of Devices and Prices (as in November 2004, all prices are in Ringgit Malaysia)

Device Name	Price (RM)
D-Link Wireless-G AP Router with 4-Port Switch DI-624+	365
D-Link Wireless-G USB DWL-G120+	245
D-Link Wireless-G PCI DWL-G520+	245
D-Link Wireless-G PCMCIA DWL-G620+	235
LinkSys Wireless Access Point Router with 4-Port Switch	220
LinkSys Wireless Access Point	230
LinkSys Wireless PCI Network Controller	170
LinkSys Wireless USB Network Controller	175
LinkSys Wireless PCMCIA Network Controller	100
PROLINK Wireless PCMCIA Network Adapter	75
PROLINK Wireless USB Adapter	100
Netgear Wireless-G AP Router with 4-Port Switch	250
Netgear Wireless-G USB Adapter	200
Netgear Wireless-G PCI Card	180
Netgear Wireless-G PCMCIA	170
SMC Wireless Access Point 2671W	180
SMC Wireless PCMCIA (EZ Connect) Network Controller	75
3COM Office Connect Wireless PCMCIA Card	110
3COM Office Connect Wireless USB Adapter	150
Aztech Wireless PCMCIA Network Card	85

Table B-1: Wireless Devices and Price List

APPENDIX C

WIRELESS LAN CONFIGURATION TO PC AND PDA

Steps to configure wireless LAN to a PC

A. Wireless LAN card Configuration:

1. Install wireless LAN card driver to your PC by following the installation guide of the Wireless LAN card.
2. Insert the wireless LAN card to your PC. Confirm that it is inserted firmly to PC.
3. Enable wireless LAN function by turning on the switch in case of using PC/PDA with built-in wireless LAN card. Consult PC/PDA guide document in detail.

B. Wireless LAN Connection:

1. Select “Control Panel” from “Start” menu.
2. Double click “Network Connections”.

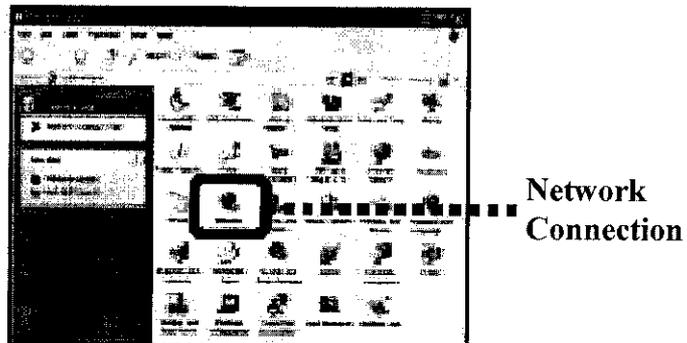


Figure C-1: “Network Connections” icon

3. After “Network Connections” window appears, right-click “Wireless Network Connection” and select “Properties”.

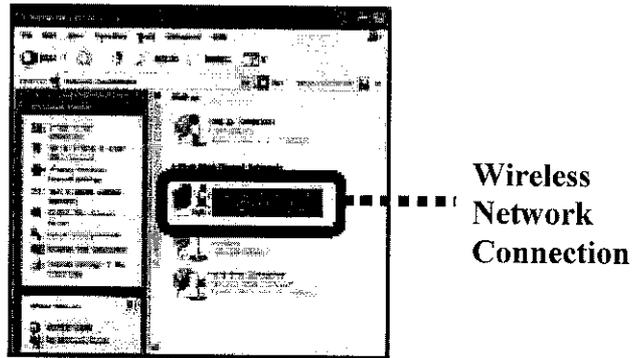


Figure C-2: “Wireless Network Connection” icon

4. After “Wireless Network Connection Properties” window appears, select “Wireless Networks” tab.
5. Check “Use Windows to configure my wireless network settings” and click “Add” button in “Preferred Networks”.
6. Click “Add” button.
 - * If "Wireless Networks" tab doesn't appear, please find "Wireless Zero Configuration" property: it is found by selecting "Control Panel" -> "Administrative" -> "Tools Services". Then please confirm "Startup type" is "Automatic", and change "Service status" to "Started".

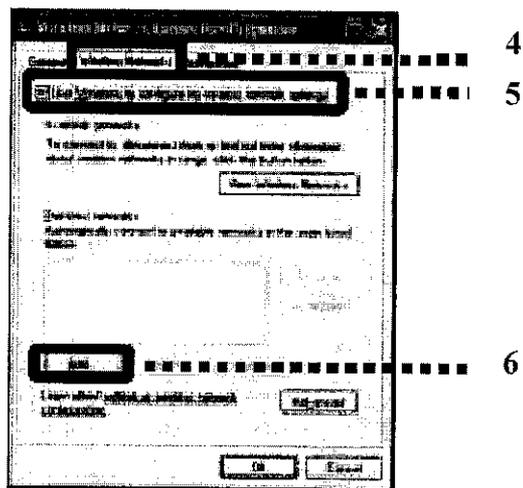


Figure C-3: “Wireless Network Connection Properties” window

7. After “Wireless Network Properties” window appears, select “Association” tab and input “Network name (SS-ID)” as notified at the registration.

8. Select “Open” for “Network Authentication” and “WEP” for “Data Encryption”.
9. Uncheck “The key is provided for me automatically”.
10. Input WEP key in “Network key” and “Confirm network key” as instructed at the registration.

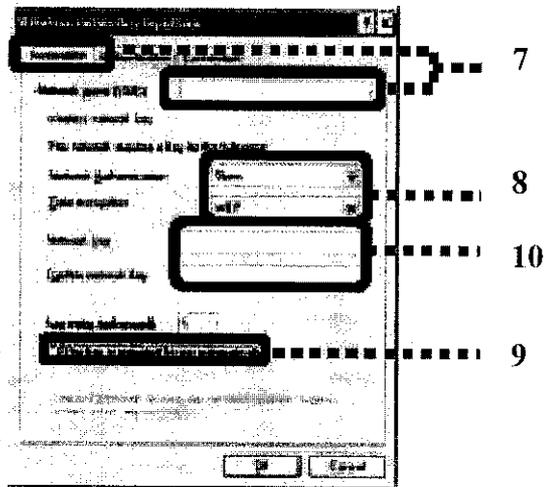


Figure C-4: “Wireless Network Properties” window

11. Select “Authentication” tab.
12. Uncheck “Enable IEEE802.1x authentication for this network”.
13. Click “OK” button.

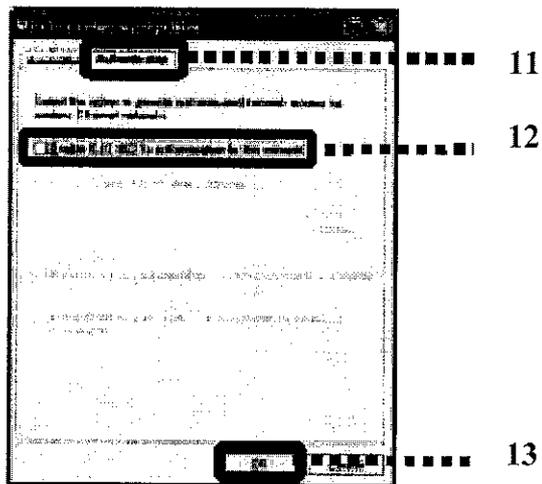


Figure C-5: “Authentication” tab under “Wireless Network Properties” window

C. Network Configuration (This part is specific to Window XP):

1. Select “General” tab on “Wireless Network Connection Properties”.

2. Select “Internet Protocol (TCP/IP)” and click “Properties” button.

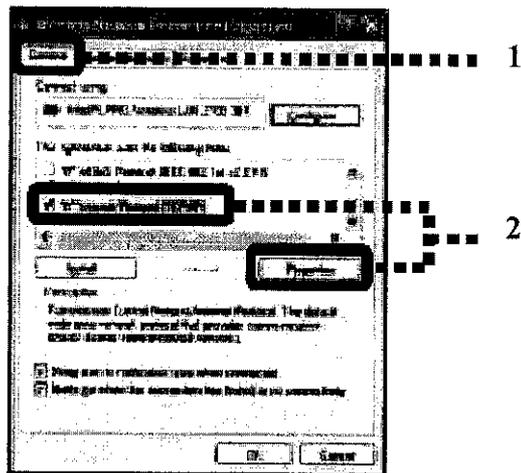


Figure C-6: “Internet Protocol (TCP/IP)” menu

3. After “Internet Protocol (TCP/IP) Properties” window appears, select “Obtain an IP address automatically” and “Obtain DNS server address automatically”.
4. Click “Advanced” button.

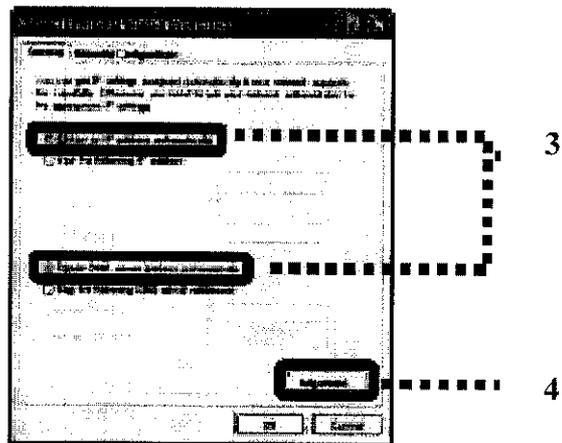


Figure C-7: “Internet Protocol (TCP/IP) Properties” window

5. After “Advanced TCP/IP Settings” window appears, select “IP Settings” tab.
6. Confirm “IP Address” field is “DHCP enabled” and “Default Gateway” field is empty.
7. Click “OK” button in this window and all the previously opened windows.

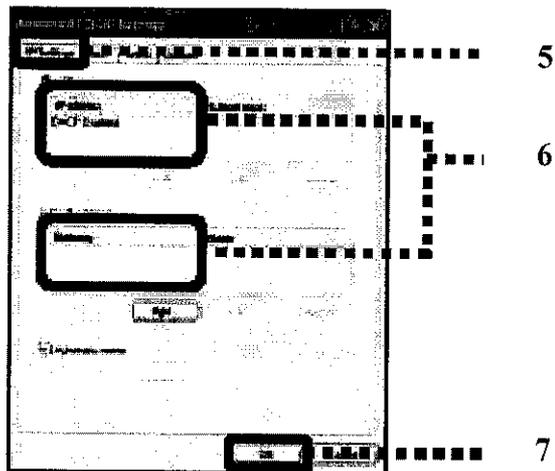


Figure C-8: “Advanced TCP/IP Settings” window

D. Web Browser Configuration (This part is specific to Internet Explorer):

1. Right-click the icon of Internet Explorer and select “Properties”. (Or load Internet Explorer and select the “Internet Options” on the “Tool” menu.)
2. After “Internet Properties” window appears, click “Connections” tab.
3. Select “Never dial a connection” in “Dial-up and Private Network settings”.
4. Click “LAN Settings”.

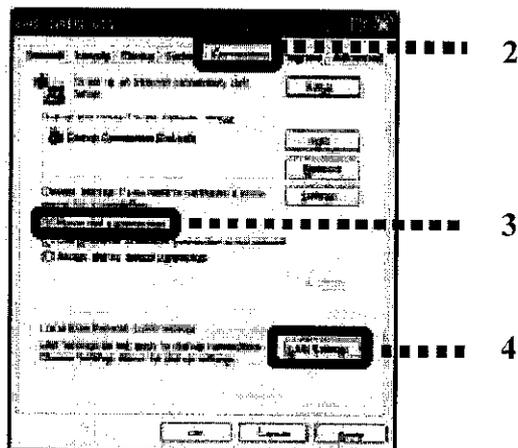


Figure C-9: “Connections” tab under “Internet Properties” window

5. After “Local Area Network (LAN) Settings” window appears, uncheck all the checkboxes of “Automatic Configuration” and “Proxy Server”.
6. Click “OK” button in this window, and “Internet Properties” window.

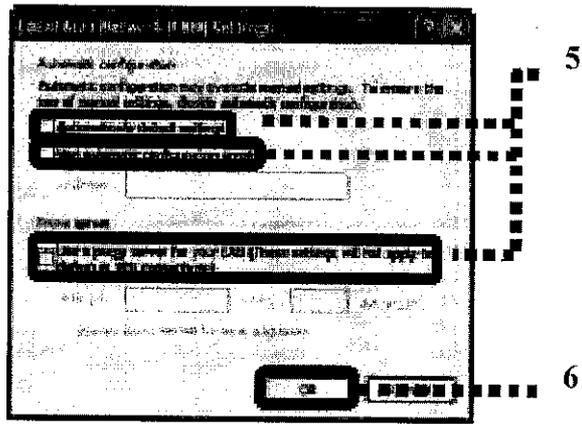


Figure C-10: “Local Area Network (LAN) Settings” window

7. Load Internet Explorer. You are now should be able to access the Internet.

Steps to configure wireless LAN to a PDA

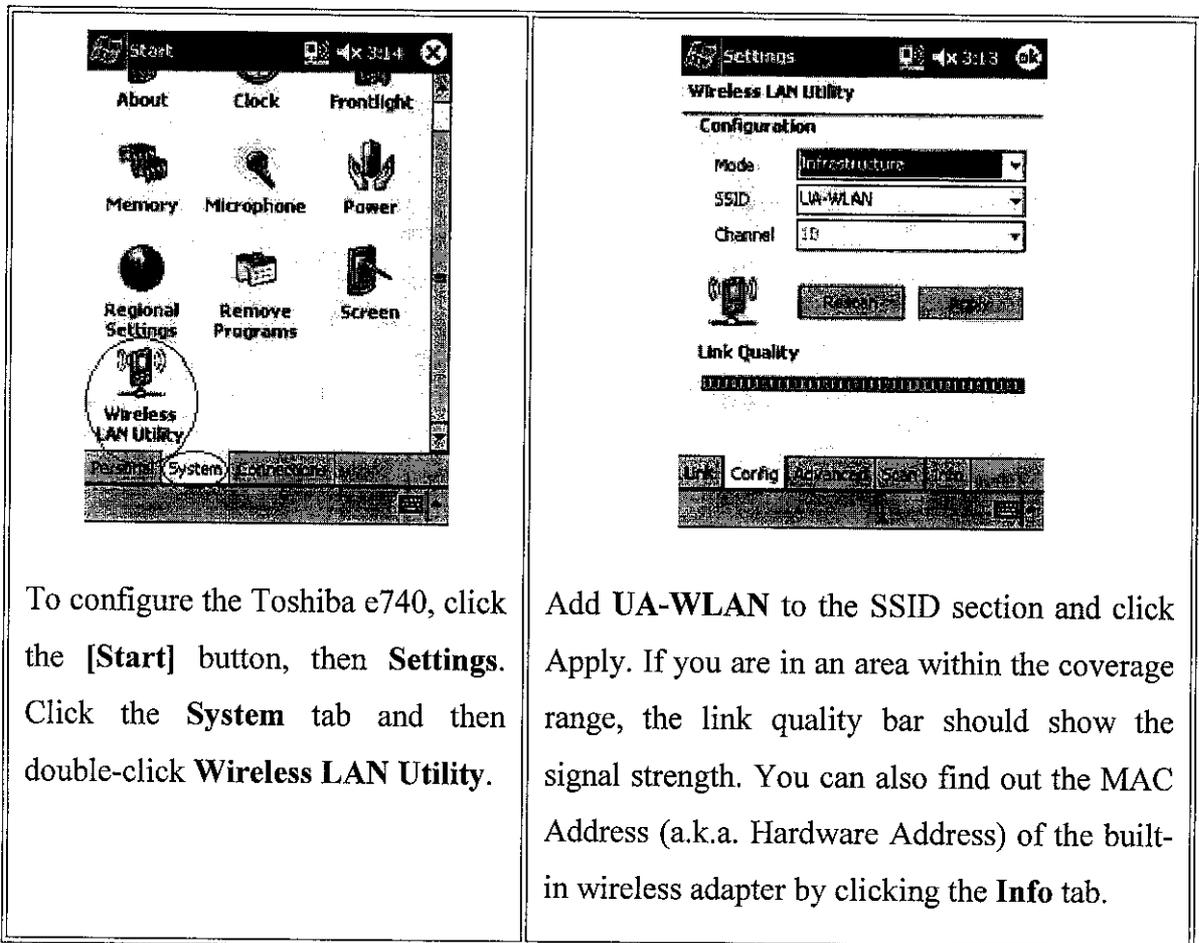
Wireless network connection hardware and methods vary from device to device. Some Pocket PC 2002 devices have built-in wireless capability and some require an outboard module. Refer to your PDA's documentation as necessary.

Connecting to the wireless network via WiFi:

1. The first step to getting connected is to open the configuration software of your wireless PDA. The primary piece of information needed here is the network name (the Service Set Identifier or SSID). The SSID of the UA wireless network is: **UA-WLAN** (note: this is case sensitive). The software for your wireless PDA will indicate successful connection to the wireless network.
2. The second step is to launch a web browser such as Internet Explorer or EudoraWeb. When you attempt to open a web page, the browser will display the IP-Nexus login page and prompt for your UARK username and password. To prevent problems with the cached information, it is recommended that you point your web browser to: <http://ipnexus.uark.edu> to log in since that is a site to which you would not otherwise be browsing. Once authenticated, you should be able to use any network and Internet associated applications such as web browsers and e-mail clients.

3. If you receive an error dialogue that the connection could not be made, click the settings button that is part of the dialogue and try changing it to "**Work Settings**" for all three drop-down menus.

For example, the following screens illustrate connecting with a Toshiba e740 Pocket PC with built-in wireless capabilities:



To configure the Toshiba e740, click the **[Start]** button, then **Settings**. Click the **System** tab and then double-click **Wireless LAN Utility**.

Add **UA-WLAN** to the SSID section and click **Apply**. If you are in an area within the coverage range, the link quality bar should show the signal strength. You can also find out the MAC Address (a.k.a. Hardware Address) of the built-in wireless adapter by clicking the **Info** tab.

Figure C-11: Toshiba e740 Pocket PC with built-in wireless capabilities configuration

Connecting from a Palm Pilot "m" series using the Xircom Wireless LAN Module

When you snap on the Xircom unit, it will automatically install the necessary driver software and start the connection dialogue which is the same as when you click the XircomPWE icon in the Home folder. It is recommended that you have a Palm Compatible Web browser installed before setting up your connection.

1. Select "Client Settings."

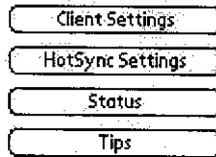


Figure C-12: Wireless Configuration Menu

2. When prompted for Profile #1 enters: **UA-WLAN** in all capital letters for the SSID. Click OK. A Confirmation screen should open. Click OK.

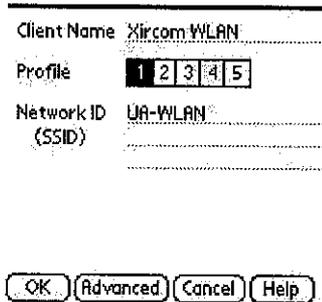


Figure C-13: "Profile" window

3. Click the **Home** button  and select **Prefs**.

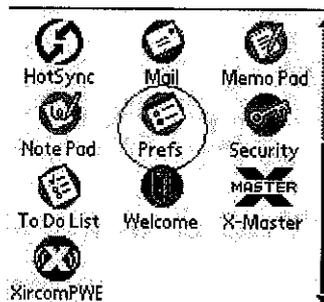


Figure C-14: Menu window

4. Click the options dropdown menu in the upper right corner to select the Network preferences.



Figure C-15: “Network Preferences” drop down menu

5. Click the Menu Button  to create a new service. Name the service: **UA**
Enter your username and password and select the **Xircom WLAN** option from the list of connections.

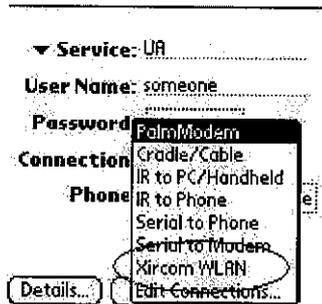


Figure C-16: “New Service” properties

6. To verify it is functioning properly, click the **Connect** button. You will need to install a **palm compatible web browser** before continuing to the next step.

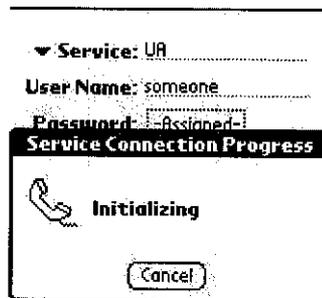


Figure C-17: “Service Connection Progress” prompt window

7. Open your web browsing program. Enter: <http://ipnexus.uark.edu> in the address bar and visit the location.
8. Enter your **UARK** username and password then click **Login**. You should receive a confirmation screen.



Figure C-18: "Login Confirmation" window

9. Now open a connection to a website and **visit location**; you should connect properly to the site.



Figure C-19: Browser window

APPENDIX D

NETWORK SIMULATION V2 CODING

Filename: mobile_network_final.tcl

```
# =====
# Define options
# =====
set val(chan)          Channel/WirelessChannel    ;#Channel Type
set val(prop)          Propagation/TwoRayGround   ;# radio-propagation model
set val(netif)         Phy/WirelessPhy           ;# network interface type
set val(mac)           Mac/802_11                ;# MAC type
set val(ifq)           Queue/DropTail/PriQueue    ;# interface queue type
set val(ll)            LL                          ;# link layer type
set val(ant)           Antenna/OmniAntenna       ;# antenna model
set val(ifqlen)        50                         ;# max packet in ifq
set val(nn)            8                          ;# number of mobilenodes
set val(rp)            DSDV                       ;# routing protocol
set val(x)             200
set val(y)             100

# =====
# Main Program
# =====

# Initialize Global Variables
set ns_                 [new Simulator]

# create trace object for ns and nam
set tracefd             [open mobile_network.tr w]
$ns_ trace-all $tracefd

set namtrace            [open mobile_network.nam w]
$ns_ namtrace-all-wireless $namtrace $val(x) $val(y)

# set up topography object
set topo                [new Topography]

$topo load_flatgrid $val(x) $val(y)

# Create God
create-god $val(nn)

# Create channel
set chan_1_             [new $val(chan)]
set chan_2_             [new $val(chan)]
```

```

set chan_3_ [new $val(chan)]
set chan_4_ [new $val(chan)]
set chan_5_ [new $val(chan)]
set chan_6_ [new $val(chan)]
set chan_7_ [new $val(chan)]
set chan_8_ [new $val(chan)]

# Create node(0) "attached" to channel #1

# configure node, please note the change below.
$ns_ node-config -adhocRouting $val(rp) \
                -llType $val(ll) \
                -macType $val(mac) \
                -ifqType $val(ifq) \
                -ifqLen $val(ifqlen) \
                -antType $val(ant) \
                -propType $val(prop) \
                -phyType $val(netif) \
                -topoInstance $topo \
                -agentTrace ON \
                -routerTrace ON \
                -macTrace ON \
                -movementTrace OFF \
                -channel $chan_1_

set node_(0) [$ns_ node]
set node_(1) [$ns_ node]
set node_(2) [$ns_ node]
set node_(3) [$ns_ node]
set node_(4) [$ns_ node]
set node_(5) [$ns_ node]
set node_(6) [$ns_ node]
set node_(7) [$ns_ node]

#disable random motion

$node_(0) random-motion 0
$node_(1) random-motion 0
$node_(2) random-motion 0
$node_(3) random-motion 0
$node_(4) random-motion 0
$node_(5) random-motion 0
$node_(6) random-motion 0
$node_(7) random-motion 0

for {set i 0} {$i < $val(nn)} {incr i} {
    $ns_ initial_node_pos $node_($i) 20
}

```

```

=====
# Provide initial (X,Y, for now Z=0) co-ordinates for mobilenodes
=====
$node_(0) set X_ 50.0
$node_(0) set Y_ 50.0
$node_(0) set Z_ 0.0

$node_(1) set X_ 0.0
$node_(1) set Y_ 0.0
$node_(1) set Z_ 0.0

$node_(2) set X_ 10.0
$node_(2) set Y_ 20.0
$node_(2) set Z_ 0.0

$node_(3) set X_ 1.0
$node_(3) set Y_ 1.0
$node_(3) set Z_ 0.0

$node_(4) set X_ 5.0
$node_(4) set Y_ 70.0
$node_(4) set Z_ 0.0

$node_(5) set X_ 50.0
$node_(5) set Y_ 70.0
$node_(5) set Z_ 0.0

$node_(6) set X_ 50.0
$node_(6) set Y_ 20.0
$node_(6) set Z_ 0.0

$node_(7) set X_ 130.0
$node_(7) set Y_ 97.0
$node_(7) set Z_ 0.0

# Node_(1), node_(2), node_(5), and node_(6) starts to move towards node_(0)
# node_(3), node_(4), and node_(7) remains at their places

$ns_ at 0.0 "$node_(0) setdest 50.0 50.0 0.0"
$ns_ at 2.0 "$node_(1) setdest 25.0 14.0 5.0"
$ns_ at 3.0 "$node_(2) setdest 10.0 25.0 5.0"
$ns_ at 0.0 "$node_(3) setdest 1.0 1.0 5.0"
$ns_ at 0.0 "$node_(4) setdest 5.0 70.0 5.0"
$ns_ at 3.0 "$node_(5) setdest 30.0 90.0 5.0"
$ns_ at 0.0 "$node_(6) setdest 30.0 2.0 5.0"
$ns_ at 0.0 "$node_(7) setdest 130.0 97.0 0.0"

```

```

# Node_(1) then starts to move away from node_(0)
$ns_ at 5.0 "$node_(1) setdest 170.0 18.0 27.0"

# Node_(2) then starts to move away from node_(0)
$ns_ at 10.0 "$node_(2) setdest 190.0 95.0 70.0"

# Node_(5) then starts to move away from node_(0)
$ns_ at 13.0 "$node_(5) setdest 50.0 90.0 33.0"

# Node_(6) then starts to move away from node_(0)
$ns_ at 18.0 "$node_(6) setdest 60.0 1.0 87.0"

#=====
# Setup traffic flow between nodes
#=====
# TCP connections between node_(0) and node_(1)

set tcp [new Agent/TCP]
$tcp set class_ 2
set sink [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp
$ns_ attach-agent $node_(1) $sink
$ns_ connect $tcp $sink
set ftp [new Application/FTP]
$ftp attach-agent $tcp
$ns_ at 3.0 "$ftp start"

# TCP connections between node_(0) and node_(2)

set tcp2 [new Agent/TCP]
$tcp2 set class_ 2
set sink2 [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp2
$ns_ attach-agent $node_(2) $sink2
$ns_ connect $tcp2 $sink2
set ftp2 [new Application/FTP]
$ftp2 attach-agent $tcp2
$ns_ at 4.0 "$ftp2 start"

# TCP connections between node_(0) and node_(3)

set tcp3 [new Agent/TCP]
$tcp3 set class_ 2
set sink3 [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp3
$ns_ attach-agent $node_(3) $sink3
$ns_ connect $tcp3 $sink3
set ftp3 [new Application/FTP]

```

```

$ftp3 attach-agent $tcp3
$ns_ at 5.0 "$ftp3 start"

# TCP connections between node_(0) and node_(4)

set tcp4 [new Agent/TCP]
$tcp4 set class_ 2
set sink4 [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp4
$ns_ attach-agent $node_(4) $sink4
$ns_ connect $tcp4 $sink4
set ftp4 [new Application/FTP]
$ftp4 attach-agent $tcp4
$ns_ at 6.0 "$ftp4 start"

# TCP connections between node_(0) and node_(5)

set tcp5 [new Agent/TCP]
$tcp5 set class_ 2
set sink5 [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp5
$ns_ attach-agent $node_(5) $sink5
$ns_ connect $tcp5 $sink5
set ftp5 [new Application/FTP]
$ftp5 attach-agent $tcp5
$ns_ at 7.0 "$ftp5 start"

# TCP connections between node_(0) and node_(6)

set tcp6 [new Agent/TCP]
$tcp6 set class_ 2
set sink6 [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp6
$ns_ attach-agent $node_(6) $sink6
$ns_ connect $tcp6 $sink6
set ftp6 [new Application/FTP]
$ftp6 attach-agent $tcp6
$ns_ at 8.0 "$ftp6 start"

# TCP connections between node_(0) and node_(7)

set tcp7 [new Agent/TCP]
$tcp7 set class_ 2
set sink7 [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp7
$ns_ attach-agent $node_(7) $sink7
$ns_ connect $tcp7 $sink7
set ftp7 [new Application/FTP]

```

```

$ftp7 attach-agent $tcp7
$ns_ at 10.0 "$ftp7 start"

#=====
# Tell nodes when the simulation ends
#=====

for {set i 0} {$i < $val(nn) } {incr i} {
    $ns_ at 25.0 "$node_($i) reset";
}
$ns_ at 25.0 "stop"
$ns_ at 25.01 "puts \"NS EXITING...\" ; $ns_ halt"
proc stop {} {
    global ns_ tracefd
    $ns_ flush-trace
    close $tracefd
}

puts "Starting Simulation..."
$ns_ run

```

APPENDIX E

INTRODUCTION TO NETWORK SIMULATOR (ns) VER. 2

Introduction to ns-2

Ns-2 is an object-oriented simulator developed as part of the VINT project at the University of California in Berkeley. The project is funded by DARPA in collaboration with XEROX Palo Alto Research Center (PARC) and Lawrence Berkeley National Laboratory (LBNL).

ns-2 is extensively used by the networking research community. It provides substantial support for simulation of TCP, routing, multicast protocols over wired and wireless (local and satellite) networks, etc. The simulator is event-driven and runs in a non-realtime fashion. It consists of C++ core methods and uses **Tcl** and **Object Tcl** shell as interface allowing the input file (simulation script) to describe the model to simulate.

Users can define arbitrary network topologies composed of nodes, routers, links and shared media. A rich set of protocol objects can then be attached to nodes, usually as **agents**. The simulator suite also includes a graphical visualizer called network animator (**nam**) to assist the users get more insights about their simulation by visualizing packet trace data.

Documentation

- ns manual available at <http://www.isi.edu/nsnam/ns/ns-documentation.html>
- ns tutorial available at <http://www.isi.edu/nsnam/ns/tutorial/index.html>

Setup

Type **extras ns2** in a terminal, and you'll get the ns2 bin directory added (temporarily) to your path or add **extras ns2** to your **.cshrc** file to have it added permanently. Alternatively, modify your PATH variable to contain

`/home/csunix/extras/ns2/current/bin/`

If you have not already done so, create a new directory in your Linux/Windows filestore to hold your practical. Move into your newly created directory.

Building ns-2 (This article is available at <http://www.isi.edu>)

Where to Start

What hardware is needed? To build ns you need a computer and a C++ compiler. We develop ns on several kinds of UNIX (FreeBSD, Linux, SunOS, and Solaris), so it installs smoothest there, but it should run on a Posix-like computer, possibly with some tweaking. Ns also build and run under Windows, see the notes below for details. Simple scenarios should run on any reasonable machine, but very large scenarios benefit from large amounts of memory.

Ns is fairly large. The all-in-one package requires about 250MB of disk space to build. Building ns from pieces can save some disk space. (If multiple people want to share files in the ns build tree to save space, you may download a simple Perl script, then follow the instruction in its README. There is detailed instruction from CS599b class of USC. You may also find discussions in the ns-users mailing list archive useful.)

How do I get the software? There are two ways to build ns: from all the pieces or all at once. If you just want to try it out quickly, you might try all at once. If you want to do C-level development, or save download time or disk space, or have trouble with all-in-one you should build it from the pieces.

ns is available both by HTTP (at the links below, all in <http://www.isi.edu/nsnam/dist/>), by anonymous FTP at <ftp://ftp.isi.edu/nsnam>, and by anonymous CVS (as described on [the anon-cvs page](#)). The ftp part of ns is mirrored in Europe at <ftp://ftp.ee.surrey.ac.uk/pub/Mirrors/ftp.isi.edu/nsnam>.

TIPS for building ns on windows:

- Instructions to build *ns* under Cygwin for win9x/2000/XP available at <http://www.isi.edu/nsnam/ns/ns-cygwin.html>
- Installation details for win95/98/2000/NT platforms available at <http://www.isi.edu/nsnam/ns/ns-win32-build.html>
- More instructions for building *ns* on Windows ME and Windows 2000 available at <http://www.public.iastate.edu/~magico/nsFiles/InstallNS1.html>
- Pre-built binaries for Windows are available for downloading from our distribution available at <http://www.isi.edu/nsnam/dist/binary/>

Important:

Please note that the release version of ns-2.26 (and nam-1.9) and above have been tested and validated under cygwin. We did not test it to build/validate under windows using visual C++. There are binaries available for ns and nam under cygwin for the current release.

Getting the Pieces

Important: *Please check the bug fixes after you finish installation!*

Ns depends on several externally available components. Below is a summary of where to get them and where they may already be (if you're a VINT developer). Since the components depend on each other, you should build them in the listed order.

Ns is developed primarily on UNIX (SunOS, FreeBSD, and Linux) and should build on most other versions of UNIX. Ns should also build under Windows-95/98/2000/NT.

Tcl/Tk

Download source:

- A modestly up to date Tcl/Tk version Tcl-8.4.5 Tk-8.4.5
- Web page: Scriptics Tcl/Tk resources available at <http://www.scriptics.com/resource/software/tcltk>. Note that while more

up to date versions of tcl/tk are available, we have not tested with them (although we expect them to work).

otcl

Download source:

- version 1.8 (released Jan 9, 2004) available at http://sourceforge.net/project/showfiles.php?group_id=30174
- daily snapshot available at <http://otcl-tclcl.sourceforge.net/tarballs/otcl-current.tar.gz>
- anonymous CVS (package "otcl") available at <http://www.isi.edu/nsnam/ns/ns-anoncvs.html#packages>
- Web page: <http://otcl-tclcl.sourceforge.net/otcl/>.

TclCL (the package formerly known as libTcl)

Download source:

- The latest version [tclcl-1.15](#) (released Jan 9, 2004)
- [daily snapshot](#)
- [anonymous CVS](#) (package "tclcl")
- web page: <http://otcl-tclcl.sourceforge.net/tclcl/>.

ns-2

Download source:

- most recent release (ns-2.27 released Jan 18, 2004), available at <http://www.isi.edu/nsnam/dist/ns-src-2.27.tar.gz>
- daily snapshot, available at <http://www.isi.edu/nsnam/dist/ns-src-snapshot.tar.gz>
- anonymous cvs (package "ns-2"), available at <http://www.isi.edu/nsnam/ns/ns-anoncvs.html#packages>
- web page: <http://www.isi.edu/nsnam/ns/>.

Pre-built binaries for the current release of ns-2.27 to run under cygwin for windows9x/2000/XP and instructions to build the cygwin environment are available from the cygwin page .

There may be known problems with the current version of ns; please check the ns installation problems web page for patches.

nam-1 (optional)

Download source:

- most recent release (nam-1.10 released Jan 18, 2004), available at <http://www.isi.edu/nsnam/dist/nam-src-1.10.tar.gz>
- daily snapshot, available at <http://www.isi.edu/nsnam/dist/nam-src-snapshot.tar.gz>
- anonymous cvs (package "nam-1"), available at <http://www.isi.edu/nsnam/ns/ns-anoncvs.html#packages>
- web page: <http://www.isi.edu/nsnam/nam/>

Pre-built binaries for nam-1.10 to run under cygwin for windows9x/2000/XP and instructions to build the cygwin environment are available from the cygwin page . You can find pre-built binary for Linux at <http://www.isi.edu/nsnam/dist/binary/nam-1.10-linux-i386.tar.gz>

Xgraph (optional, but needed for test suites)

Download source: version 12.1, or by anonymous cvs (package "xgraph"). Web page: <http://www.isi.edu/nsnam/xgraph/>.

(This version is maintained by the ns maintainers and includes portability fixes over the older 12.0 release.)

Perl (optional, but needed for test suites)

Download source: latest stable release; web page: <http://language.perl.com/>

Note that version 5.003 or later is required.

Tcl-debug (optional, available for Tcl debugging help)

Download source: version 1.7; web page: <http://expect.nist.gov/tcl-debug/> This version will work with Tcl/Tk 8.0 release.

dmalloc (optional, available for memory debugging)

Download source: version 4.8.0. Web page: <http://www.dmalloc.com/>; specify `-with-dmalloc` during configure to include.

sgb2ns conversion program (optional, needed to convert GT-ITM output to ns-2 format)

Download source: sgb2ns conversion program. For more info on GT-ITM topology generators see GT-ITM Topology Generator at <http://www.isi.edu/nsnam/ns/ns-topogen.html#gt-itm>

tiers2ns conversion program (optional, needed to convert Tiers output to ns-2 format)

Download source: tiers2ns.awk. For more info on Tiers topology generators see Tiers Topology Generator at <http://www.isi.edu/nsnam/ns/ns-topogen.html#tiers>

Cweb and sgb source code (optional, required to create sgb-library that is used by gt-itm and sgb2ns programs)

Download cweb source from cweb ftp page available at <ftp://labrea.stanford.edu/pub/cweb/cweb3.4g.tar.gz>

Download sgb source code from sgb ftp page available at <ftp://labrea.stanford.edu/pub/sgb/sgb.tar.gz>

VINT developers at ISI can find all of these packages in `/nfs/filb2/public/pkgs`.

Building it From Sources

- Fetch the source code as described above.
- Unpack OTcl, TclCL and ns source into the same top level directory.
- build OTcl, TclCL and ns

For UNIX:

- cd into the OTcl directory
- run *./configure*
- run *make*
- cd into the TclCL directory
- run *./configure*
- run *make*
- cd into the ns directory
- run *./configure*
- run *make*

For UNIX, a simple *./configure* will try to auto-detect the packages ns needs to build. Auto-detection search sensible places (like /usr/local) and the directory above current directory. If you have packages installed elsewhere you can explicitly tell ns where something is with options like *--with-tcl=/your/path/to/tcl*. Run *./configure --help* for a complete list of options.

For Windows 95/98/2000/NT:

You can either build it easily straight out-of-the-box by building under cygwin or can build using Microsoft Visual C++. See the *cygwin-build* page for instructions to build under cygwin for win9x/2000/XP. Or look at *win32-build* page for details on installation on win95/98/2000/NT platforms using visual C++.

Since we have tested the current release of ns/nam under cygwin only we do not have any binaries available for visual C++ build for this release.

Important: the primary ns build platform are various flavors of Unix. However, because the primary ns developers don't regularly use it there and we can't automate things on Windows as well as on UNIX, build problems on Windows are more frequent. We welcome patches from windows users to correct any problems.

- To build under cygwin, you need to follow exactly the same instructions as provided for building under unix (see above paragraph).
- To build under windows (using visual C++) do the following. Run `vcvars32.bat` in `$YOUR_VC_PATH/bin` to setup pathnames for your VC executables. **Not** if it complains about limited environment space, add the following line into your `autoexec.bat` for win95/98, (if you are using NT, add that to your system profile accessible from Control Panel) `SHELL= C:\COMMAND.COM C:\ /E:32000 /P` You also can change 32000 to smaller or larger values. (By [Ling Su](#))
- cd into the TclCL directory
- **Important** Look at the pathnames for VC++ in `conf/makefile.win`. If they do not match what's in your system, correct them. Also look at other pathnames in that file, e.g., for Tcl/TK and OTcl, set them to the correct one.
- run `nmake /f makefile.vc`
- cd into the ns directory
- Do the same pathname check in `conf/makefile.win`. This time also checks TclCL's pathname.
- run `nmake /f makefile.vc`
- Verify that it built correctly and runs:
 - `./validate`

Getting everything at once

Ns-all-in-one is a package which contains required components and some of optional components used in running ns. The package contains an "install" script to automatically configure, compile and install these components. After downloading, run the install script. If you haven't installed ns before and want to quickly try ns out, ns-all-in-one may be easier than getting all the pieces by hand.

Currently the package contains:

- Tcl release 8.4.5 (required component)

- Tk release 8.4.5 (required component)
- Otcl release 1.8 (required component)
- TclCL release 1.15 (required component)
- Ns release 2.27 (required component)
- Nam release 1.10 (optional component)
- Xgraph version 12 (optional component)
- CWeb version 3.4g (optional component)
- SGB version 1.0 (?) (optional component, builds sgblib for all UNIX type platforms)
- Gt-itm gt-itm and sgb2ns 1.1 (optional component)
- Zlib version 1.1.4 (optional, but required should Nam be used)

Currently, ns-all-in-one works on UNIX systems and under cygwin for windows 9x/2000/XP. If you need to build ns under Windows (using visual C++), or if you have problems with all-in-one, we encourage you to build it from its pieces.

Download source:

- current release 2.27 (released Jan 18, 2004), available at <http://www.isi.edu/nsnam/dist/ns-allinone-2.27.tar.gz>

Important: *Please check the bug fixes after you finish installation!* .

Getting Older Versions of Ns

Q: The current version of ns has too many features and fixed bugs... I want a more challenging network simulator. (Or, more likely, I have someone else's code that was built against an old ns release.)

A: All available releases of ns-2 and nam are at our web and ftp sites. Please note that many of these versions have known bugs---we can only support the most recent ns release.

Where to go from here?

If you have problems building ns, try reading the Installation Problems and Bug Fixes Web Page, available at <http://www.isi.edu/nsnam/ns/ns-problems.html>

If you want to write new simulation scripts or modules, please check out the documentation links on the main ns page.

Now that ns runs, you might want to consider some tips about debugging your ns scripts.

If you plan on modifying ns itself you should do a `make depend` to add dependency information to configure's Makefile.

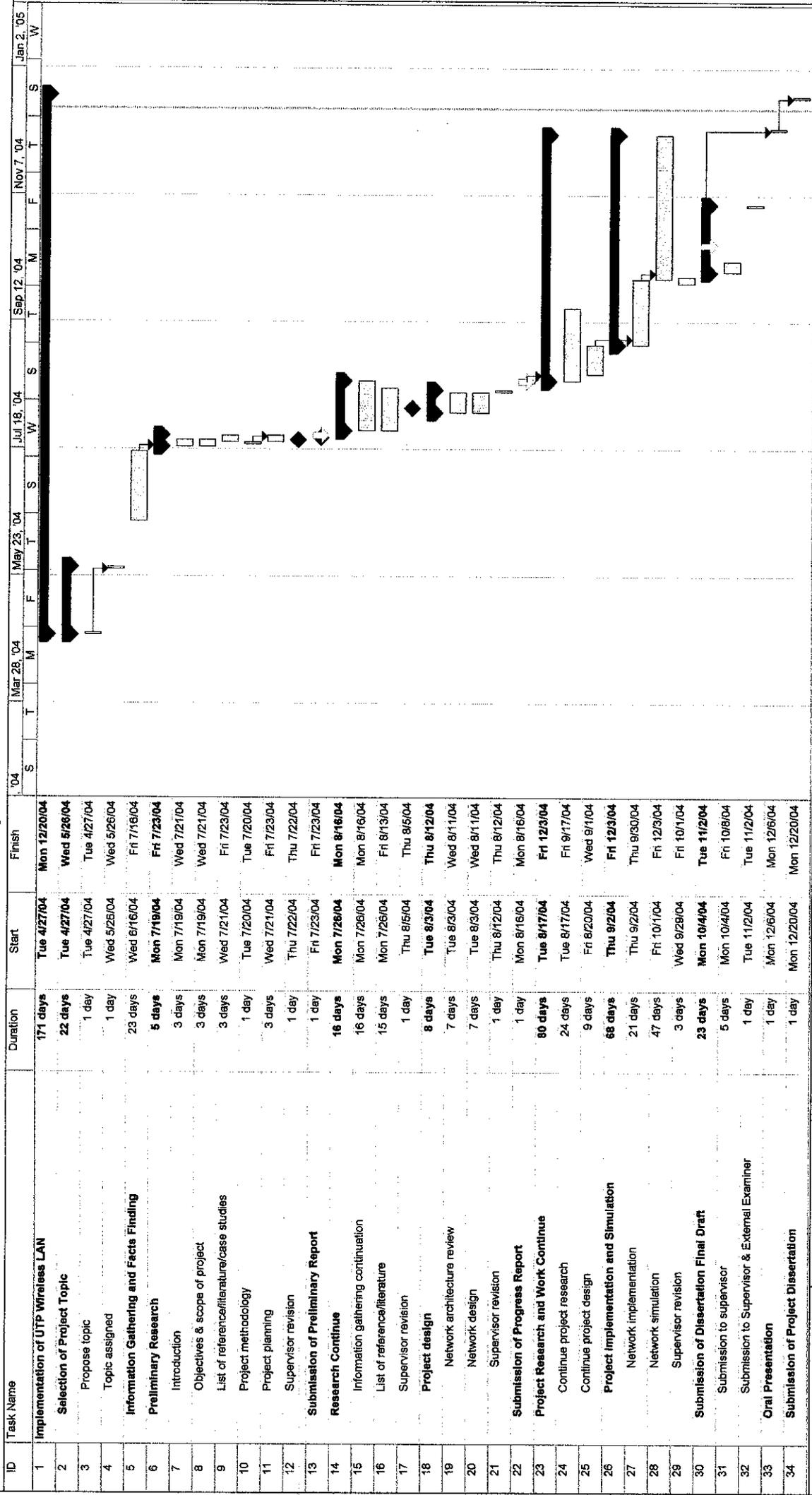
To animate your simulations, you might want to examine nam, the network animator.

APPENDIX F

PROJECT SCHEDULE

Figure F-1: Project Schedule
(as shown on the next page)

Project Schedule: Implementation of Wireless LAN in UTP



Project: FYP Schedule
Date: Wed 12/15/04

█ Task
█ Progress
◆ Milestone
█ Summary
█ External Tasks
◆ External Milestones
█ Deadline

APPENDIX G

GLOSSARY

A

AES – Advanced Encryption Standard. A symmetric key encryption technique which will replace the commonly used DES standard. It was the result of a worldwide call for submissions of encryption algorithms issued by NIST in 1997 and completed in 2000. The winning algorithm, Rijndael, was developed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen. AES provides strong encryption in various environments: standard software platforms, limited space environments, and hardware implementations.

AP – Access Point. A base station in a wireless LAN. Access points are typically stand-alone devices that plug into an Ethernet hub or server. Like a cellular phone system, users can roam around with their mobile devices and be handed off from one access point to the other. A hardware device, or software used in conjunction with a computer, that serves as a communications "hub" for wireless clients and provides a connection to a wired LAN. An AP can double the range of wireless clients and provide enhanced security.

Attenuation – A reduction in strength or deterioration of an electrical signal as it passes through a transmission medium. Attenuation generally increases with frequency, cable length and the number of connections in a circuit. Attenuation is measured in decibels (dB). In optical fiber, a diminution of the signal as a function of length traveled.

Authentication – Determines a user's identity, as well as determining what a user is authorized to access. The most common form of authentication is user name and password, although this also provides the lowest level of security. VPNs use digital certificates and digital signatures to more accurately identify the user.

B

Bandwidth – The width or capacity of a communications channel. Analogue bandwidth is measured in Hertz (Hz) or cycles per second. Digital bandwidth is the amount or volume of data that may be sent through a channel, measured in bits per second, without distortion. Bandwidth should not be confused with the term "band", such as a wireless phone that operates on the 800 MHz band. Bandwidth is the space it occupies on that band. The relative importance of bandwidth in wireless communications is that the size, or bandwidth, of a channel will impact transmission speed. Lots of data flowing through a narrow channel takes longer than the same amount of data flowing through a broader channel.

Bluetooth – Chip technology enabling seamless voice and data connections between a wide range of devices through short-range digital two-way radio. It is an open specification for short-range communications of data and voice between both mobile and stationary devices. For instance, it specifies how mobile phones, WIDs, computers and PDAs interconnect with each other, with computers, and with office or home phones.

Broadband – A transmission facility having a bandwidth sufficient to carry multiple voice, video or data channels simultaneously. Each channel occupies (is modulated to) a different frequency bandwidth on the transmission medium and is demodulated to its original frequency at the receiving end. Channels are separated by "guardbands" (empty spaces) to ensure that each channel will not interfere with its neighboring channels. This technique is used to provide 50 CATV channels on one coaxial cable.

C

CBR – Constant Bit Rate. An ATM service category which supports a constant or guaranteed rate to transport services such as video or voice as well as circuit emulation which requires rigorous timing control and performance parameters.

Client – Node or software program that is used to contact and obtain data from a server software program on another computer.

D

DHCP – 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. When a company sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer. 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. DHCP uses the concept of a ‘lease’ or amount of time that a given IP address will be valid for a computer. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DSSS – Direct-Sequence Spread Spectrum. A transmission technology used in WLAN (wireless LAN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.

E

EAP – Extensible Authentication Protocol. An optional IEEE 802.1x security feature ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server.

Eavesdropping – Observing information that was intended to be confidential. The threat to the property of privacy.

Encryption – Encryption is the transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it was not intended, including those who can see the encrypted data. Encryption may be used to make stored data private (e.g., data that is stored on a potentially vulnerable hard disk), or to allow a non-secure communications channel to serve as a private communications channel. Encryption is sometimes described as the process of converting plain text into cipher text.

F

FCC – Federal Communications Commission. The federal agency responsible for regulating broadcast and electronic communications in United States.

FHSS – Frequency Hopping Spread Spectrum. A transmission technology in which the data signal is modulated with a narrowband carrier signal that "hops" in random but in a known sequence from frequency to frequency as a function of time over a wide band of frequencies. The signal energy is spread in time domain rather than chopping each bit into small pieces in the frequency domain. This technique reduces interference because a signal from a narrowband system will only affect the spread spectrum signal if both are transmitting at the same frequency at the same time. If synchronized properly, a single logical channel is maintained.

Firewall – A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. Basically, a firewall, working closely with a router program, filters all network packets to determine whether to forward them toward their destination. A firewall is often installed away from the rest of the network so that no incoming request can get directly at private network resources. There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain names and IP addresses. For mobile users, firewalls allow remote access in to the private network by the use of secure logon procedures and authentication certificates.

G

Gateway – A computer system for exchanging information across incompatible networks by translating between two dissimilar protocols. May also be describes as any mechanism that gives access to another, such as an ISP which acts as a gateway to the Internet.

I

IEEE – Institute of Electrical and Electronics Engineers. A professional organization whose activities include the development of communication and network standards. IEEE LAN standards are the predominant LAN standards today.

L

Link layer – Also known as the data link layer. The OSI second layer which creates packets from data sent by higher layers and passes these to the physical layer.

O

OFDM – Orthogonal Frequency Division Multiplexing. Divides a range of available bandwidth spectrum into a series of frequencies known as tones. Flarion uses the 5 GHz channel and divides each channel into 400 discrete tones (each at slightly different frequency). Orthogonal tones do not interfere with each other when the peak of one tone corresponds with the null. All frequencies fade but the rapid switching, frequency-hopping technique is supposed to allow more robust data service.

P

PDA – Personal Digital Assistant. A small hand-held computer that in the most basic form, allows you to store names and addresses, prepare to-do lists, schedule appointments, keep track of projects, track expenditures, take notes, and do calculations. Depending on the model, you also may be able to send or receive e-mail; do word processing; play MP3 music files; get news, entertainment and stock quotes from the Internet; play video games; and have an integrated digital camera or GPS receiver.

Portable computer – A PC that is compact and light enough to be carried about easily, for use at different locations. Portable computers can be hand-held devices, wearable systems, or vehicle-mounted systems.

Q

QoS – Quality of Service. Network device capabilities that provide some guarantee of performance such as traffic delivery priority, speed, latency, or latency variation. Delivery of good-quality audio or video streams typically requires QoS capabilities.

R

RF – Radio Frequency. The 10 kHz to 300 GHz frequency range that can be used for wireless communication. The term RF is usually used to distinguish signals transmitted to and from the satellite from signals processed at other frequencies within the same communication system (e.g. intermediate frequencies).

Router – A device that determines the next network point to which a data packet should be forwarded enroute toward its destination. The router is connected to at least two networks and determines which way to send each data packet based on its current understanding of the state of the networks it is connected to. Routers create or maintain a table of the available routes and use this information to determine the best route for a given data packet.

S

Scalability – The ability to expand the number of users or increase the capabilities of computing solution users without making major changes to the systems or application software.

Server – Node or software program that provides services to clients.

Spectrum analyzer – An instrument which displays the frequency spectrum of an input signal, usually amplitude vertical vs. frequency horizontal.

SSH – Secure Shell. Sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted. SSH uses RSA public key cryptography for both connection and authentication. Encryption algorithms include Blowfish, DES, and IDEA. IDEA is the default.

SSID – Service set identifier. A unique identifier that stations must use to be able to communicate with an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

SSL – Secured Sockets Layer. A protocol that transmits your communications over the Internet in an encrypted form. SSL ensures that the information is sent, unchanged, only to the server you intended to send it to. Online shopping sites frequently use SSL technology to safeguard your credit card information.

T

TCP – Transmission Control Protocol. Internet networking software that controls the transmission of packets of data over the internet. Among its tasks, TCP checks for lost packets, puts the data from multiple packets into the correct order, and requests that missing or damaged packets be resent. Computers must run TCP to communicate with World Wide Web servers.

Third-Generation (3G) – In mobile telephony, third-generation protocols support much higher data rates, measured in Mbps, intended for applications other than voice. 3G networks trials started in Japan in 2001. 3G networks are expected to be starting in Europe and part of Asia/Pacific by 2002, and in the US later. 3G will support bandwidth-hungry applications such as full-motion video, video-conferencing and full Internet access. 1G, 2G, 2.5G, IMT-2000, UMTS, WCDMA, www.3gpp.org

Throughput – Throughput refers to the performance of data transmission, and is measured by characters actually transmitted or received during a certain period of time. The throughput of a connection depends on CPU, memory, performance between the two devices, pattern of measurement, as well as the performance of the operating system. Throughput is usually measured in bps (bits per second).

U

UDP – User Datagram Protocol. A connection-less, unreliable, transport protocol which provides multiplexing and error detection for applications, which require a low-cost protocol for one-shot transactions; cf. datagram, packet, TCP. Transport layer protocol in the TCP/IP protocol suite used in the Internet. UDP is used at the two ends of a data transfer. It does not establish a connection or provide reliable data transfer like TCP.

USB – Universal Serial Bus. An interface standard for connecting peripheral devices to computers. Hardware components for implementing a USB interface include connector ports on computers and cables for connecting peripheral devices to the computer. The USB standard supports data transfer rates of 12 Mbps. A single USB port can be used to connect up to 127 peripheral devices. USB is gradually replacing SCSI as the dominant peripheral interface standard.

V

VBR – Variable Bit Rate. QoS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class. VBR (RT) is used for connections in which there is a fixed timing relationship between samples. VBR (NRT) is used for connections in which there is no fixed timing relationship between samples, but that still need a guaranteed QoS.

VLAN – Virtual Local Area Network. A logical, not physical, group of devices, defined by a software. VLANs allow network administrators to re-segment their networks without physically rearranging the devices or network connections. VLANs allow departments that are dispersed at two or more locations to connect all their users to one

departmental network. This overcomes the constraint that is associated with Local Area Networks (LANs), which can only group together users who are located in the same geographical vicinity, such as a small building or one section of a building.

VPN – Virtual Private Network. A way to communicate through a dedicated server securely to a corporate network over the Internet. Windows NT, 2000 and XP offer native VPN support. Also, VPNs are recommended to secure 802.11b wireless LANs as well. VPNs send data over the public Internet through secure "tunnels."

W

WEP – Wired Equivalent Privacy. WEP data encryption is defined by the 802.11 standard to prevent (i) access to the network by "intruders" using similar wireless LAN equipment and (ii) capture of wireless LAN traffic through eavesdropping. WEP allows the administrator to define a set of respective "Keys" for each wireless network user based on a "Key String" passed through the WEP encryption algorithm. Access is denied by anyone who does not have an assigned key.

Wi-Fi – Short for wireless fidelity This is another name for IEEE 802.11b. It is a trade term promulgated by the Wireless Ethernet Compatibility Alliance (WECA). "Wi-Fi" is used in place of 802.11b in the same way that "Ethernet" is used in place of IEEE 802.3. Products certified as Wi-Fi by WECA are interoperable with each other even if they are from different manufacturers. A user with a Wi-Fi product can use any brand of Access Point with any other brand of client hardware that is built to the Wi-Fi standard.

WLAN – Wireless Local Area Networks. Operating in the 2.4 GHz and 5.8 GHz unlicensed ISM bands and using spread spectrum technology are presently under development. It is expected that data rates of 1 Mbps and 10 Mbps can be achieved at 2.4 GHz and 5.8 GHz, respectively. A WLAN standard operating at 2.4 GHz (IEEE 802.11) is being 'painfully' defined (with four different versions), while European countries are developing an alternative standard (HIPERLAN) for 10 Mbps transmission, using the 5.8 GHz band.