

**WIRELESS MONITORING SYSTEM**

**YAAKUB BIN IDRIS**

**A report submitted in partial fulfilment  
of the requirements for the award  
of the degree of  
Bachelor of Computer Science (Computer Systems & Network)**

**Faculty of Computer Systems & Software Engineering  
University College of Engineering & Technology Malaysia**

**NOVEMBER 2005**

## ABSTRACT

Nowadays, wireless technology is used widely by so many users from government, private sector and even student. These technologies are use at office, café and KUKTEM. This technology are able to be used in any stage of ages. Even without had to plug the connection to any plug, user can connect to anywhere by having a Wireless Network Interface Card. User need connect to any access point and they are connected to the world without borders. Although it's so easy to be used, but it still had some problem where it came to the usages. It do not show any information on network usage in human readable and hard to understand whether display it in Kilobyte per second (KB/s), Kilobit per second (Kb/s), packet, error, average of usage, maximum of usage, and overall total of network usage. This will cause major problem when it came to security matters. It also can cause problem where some of the user used the bandwidth and cause a heavy traffic. With the monitoring tool that will be build, this problem can be solve when it came to some problem that aren't supposed to show up. This tool can give some power to the administrator to monitor the connection to network. This are hopefully can help to solve the problem.

## ABSTRAK

Sekarang ini, teknologi tanpa wayar telah digunakan secara meluas oleh pengguna sama ada dari sektor awam, swasta dan juga pelajar. Teknologi ini digunakan di pejabat, kafeteria dan juga di KUKTEM. Teknologi ini mudah digunakan oleh pelbagai lapisan peringkat umur. Pengguna dapat menggunakan rangkaian komputer di mana sahaja tanpa perlu menyambungkan wayar pada mana-mana *port*, dengan hanya menggunakan *wireless* kad yang disambungkan pada komputer. Pengguna cuma perlu membuat sambungan kepada mana-mana *access point* dan mereka akan disambungkan ke rangkaian internet. Walaupun teknologi ini mudah digunakan, tetapi ia masih mempunyai masalah terutamanya jika melibatkan penggunaannya. Ia tidak akan memaparkan sebarang maklumat dalam bentuk berkaitan dengan penggunaan rangkaian internet dalam bentuk yang mudah difahami samada data yang dipaparkan dalam *Kilo Byte* per saat (KB/s), Kilo Bit per saat (Kb/s), paket, paket bermasalah, purata penggunaan, maksimum and jumlah keseluruhan penggunaan rangkaian. Ini merupakan masalah besar jika melibatkan tentang faktor-faktor keselamatan rangkaian. Ia juga akan menimbulkan masalah di mana jika sesetengah pengguna menggunakan lebar jalur yang tinggi dan melibatkan kesesakan pada rangkaian. Sistem yang dibangunkan dapat mengatasi masalah yang tidak sepatutnya wujud. Sistem ini dapat membantu pentadbir rangkaian untuk mengawasi sambungan ke rangkaian komputer. Ini secara langsung dapat membantu menyelesaikan permasalahan tersebut.

## TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	Title Page	i
	Declaration	ii
	Dedication	iii
	Acknowledgement	iv
	Abstract	v
	Abstrak	vi
	Table of Content	vii
	List of Figures	x
	List of Abbreviation	xii
	List of Symbols	xiii
	List of Appendix	xiv
<b>1</b>	<b>INTRODUCTION</b>	
	1.1 Introduction	1
	1.2 Problem Statement	2
	1.3 Objectives	2
	1.4 Scope	3
	1.5 Expected Result	3
	1.6 Organization of the Report	3
<b>2</b>	<b>LITERATURE REVIEW</b>	
	2.1 Introduction	4
	2.2 Wireless History	4
	2.3 Definition of Wireless LANs	5

2.4	Definition of Network Monitoring	6
2.5	Definition of Monitoring System	7
2.6	Monitoring Tools Function	7
2.7	Capturing 802.11 Traffic	7
2.8	Monitoring 802.11 Traffic	8
2.9	Analysis of Existing System	9
2.9.1	Current System Condition	9
2.9.2	Weakness of Current System	12
2.10	Proposed Solution	13
2.11	Selected Software for Development	13
2.11.1	Advantage Using <i>Ncurses</i>	13
2.11.2	Advantage Using C	16
2.11.3	GCC Compiler	16
2.17	Conclusion	17
<b>3</b>	<b>METHODOLOGY</b>	
3.1	Introduction	18
3.2	Systems Development Life Cycle (SDLC)	18
3.3	Project Identification and Selection	20
3.4	Project Initiation And Planning	21
3.5	Analysis	21
3.5.1	Requirements Determination	21
3.5.2	Analysis of Information	23
3.6	Design Stage	23
3.7	Implementation Stage	27
3.7.1	Development Stage	27
3.7.2	Testing Stage	29
3.8	Maintenance	32
3.8.1	Documentation	32
3.9	Conclusion	33
<b>4</b>	<b>RESULT AND DISCUSSION</b>	
4.1	Introduction	34

4.2	Result	34
4.2.1	Capturing Data from IP Address	35
4.2.2	Data Analyze Stage	38
4.3	Discussion	40
4.4	Conclusion	41
<b>5</b>	<b>CONCLUSION</b>	
5.1	Introduction	42
5.2	Advantage and Disadvantage	42
5.3	Further Enhancements	44
5.4	Tips for Build Other Monitoring Tools	44
5.5	Conclusion	45
	<b>REFERENCES</b>	<b>46</b>
	<b>APPENDIX A</b>	<b>47</b>

## LIST OF FIGURES

FIGURE NO	TITLE	PAGE
2.1	A wires local area network provides connectivity over the airwaves within a local area, such as building	5
2.2	Signal wave monitoring	10
2.3	Sample Kwifimanager that already exist in FEDORA	10
2.4	Signal bandwidth monitor	11
2.5	Text based display information	11
2.6	Sample output using <i>Netstat</i>	12
2.7	Sample read function key from keyboard using <i>Ncurses</i>	14
2.8	Sample management windows using <i>Ncurses</i> in Midnight Commander	15
3.1	The System Development Life Cycle stages	20
3.2	Interface for design prototype for wireless monitoring	23
3.3	Interface for design prototype for the help menu	24
3.4	Flow chart for Wireless Monitoring System	25
3.5	Sample cording for get source input	27
3.6	Sample coding for main windows	28

3.7	Sample coding for display available network devices	28
3.8	Sample coding for display data in KB, Kb, MB and GB	29
3.9	Sample output from <i>/proc/net/dev</i>	30
3.10	Sample of interface for read data	31
3.11	The result when connections are not available	31
3.12	Sample output using <i>/proc/net/dev</i>	32
4.1	Interface using input from <i>Netstat -i</i>	35
4.2	Interface using input from <i>/proc/net/dev</i>	36
4.3	Display result in KB/s	37
4.4	Display result in Kb/s	37
4.5	Display result in Packet per second	37
4.6	Display error result in second	37
4.7	Display result in average 30 second	39
4.8	Display result in maximum usage of network	39
4.9	Display result in total of network usage	39



**LIST OF ABBREVIATION**

ANSI	-	American National Standards Institute
API	-	Application Programming Interface
GUI	-	Graphical User Interface
GCC	-	GNU Compiler Collection
GTK	-	Gimp Toolkit
ICMP	-	Internet Control Message Protocol
IP	-	Internet protocol
LAN	-	Local Area Network
MAC	-	Media Access Control
NIC	-	Network Interface Card
POSIX	-	Portable Operating System Interface For UNIX
SDLC	-	Systems Development Life Cycle
SDRAM	-	Synchronous Dynamic Random Access Memory
SNMP	-	Simple Network Management Protocol
TCP	-	Transfer Control Protocol
UDP	-	User Datagram Protocol
VGA	-	Video Graphics Array

**LIST OF SYMBOLS**

GB/s	-	Gigabyte Per Second
Gb	-	Gigabyte
KB/s	-	Kilobyte Per Second
KB	-	Kilobyte
Kb/s	-	Kilobit Per Second
Kb	-	Kilobit
MB/s	-	Megabyte Per Second
MB	-	Megabyte
MHz	-	Mega Hertz

**LIST OF APPENDIX**

<b>APPENDIX</b>	<b>TITLE</b>	<b>PAGE</b>
A	Gantt Chart	47

## **CHAPTER 1**

### **INTRODUCTION**

#### **1.1 Introduction**

Nowadays the usages of the wireless monitoring system in borderless world are so important nowadays. These technologies are expanding enormously from one technology to another technology. With only a Local Area Network (LAN), it expands to Wireless Local Area Network. With only a cable connection, it now comes to the world without any cable or should we call it world without wired. Expanding so fast, this technology had to be monitored so the usages are not being misused by somebody that does not know about responsibility. It also had to be monitored to gain information about the usage of the technology.

The wireless technology is used by so many users, especially in education center where it has been the most useful technology for the students and even in office or chafe. These technologies are so easy to be used for any stage of ages. Without even had to plug the connection to any plug, user can connect to anywhere just by simply have a Wireless Network Interface Card. User had to connect to any access point and, they are connected to the world without borders.

With the Monitoring System that be build, this problem can be solve when it came to some problem that are not supposed to show up. This tool can give some power to the administrator to monitor the connection from any device that connected to access point. This are hopefully can help to solve the problem.

## 1.2 Problem Statement

They are two types of existing monitoring system in UNIX platform which is the system that has their own graphical user interface (GUI) and the other not. For system that have interface, it just only display the strength of the wireless connection and does not provide the information about the total packet being transmit and receive also bandwidth usage of network interface card.

The monitoring system that does not have interface, it displays data that being transmit and receive from the network interface card. Some of them are hard to read and the data that being capture is not in real time. The systems only display the capture packet at the event time only. This type of data cannot be analyze to make summarization for the packet that being capture.

This monitoring system that been build can solve the problem having in both system by extract out their advantage and build the new monitoring system so that the monitoring system can be reliable.

## 1.3 Objectives

The objectives of this project are:

- (a) To build a monitoring system that monitors the wireless connections using wireless network interface card.
- (b) The Wireless Monitoring System can monitor the output of network interface card in KB/s, Kb/s, packets, errors, average, maximum and total summation network usage.
- (c) The wireless monitoring system can monitor the number of packet that is transmitted and receive by each active internet protocol (IP) address by using *Ncurses* to display data in real time.

## **1.4 Scope**

The scopes for Wireless Monitoring System are:

- (a) The data from network interface card will be capture in packet.
- (b) The Wireless Monitoring System will be use in UNIX platform only.
- (c) The Wireless Monitoring System builds by adding new module and new method capturing data from wireless card to current monitoring system.
- (d) Data that is capture through wireless card presented in text in real time.

## **1.5 Expected Result**

The system that is going to be build is a system that monitors the packet that is being transmitted by an active IP address in a Wireless Local Area Network. This system monitors the packet and creates information's about the usage of the bandwidth. The monitored information's, will display output of active device in KB/s, Kb/s, packets, errors, average, maximum and total summation of network interface card. This could help the administrator to check also track down the usage of the wireless base on the IP address.

## **1.6 Organization of the Report**

This report basically is divided into five main chapters to discuss different issues related to this project. Chapter one is concentrated on the introduction, objective and scope of the project. Meanwhile chapter two will discuss the literature review about the purpose study for developing Wireless Monitoring System. The methodology of study or development will be discussed detail in chapter three. Result of the development will be discussed in chapter four and chapter five will conclude the process through along this project.

## CHAPTER 2

### LITERATURE REVIEW

#### 2.1 Introduction

In this chapter, all related issues for this project are studied. There are two main sources; books related to wireless protocol and internet resources.

#### 2.2 Wireless History

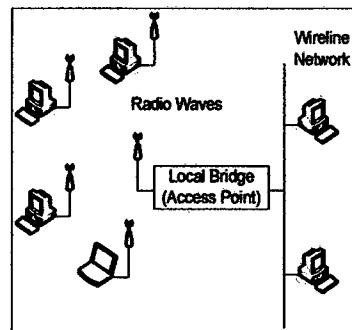
Wireless communication technologies have existed and been utilised for over a hundred years. Guglielmo Marconi, the Italian founder of wireless technologies, developed an interest in technology and communications as a child. He had read about and understood the work of Heinrich Rudolf Hertz and began to see the significance that wireless communication would have for the modern world. In 1894 Marconi began experimentations, and in 1899 sent a telegraphic message across the English Channel, without needing to use wires (Jeffrey. *et al*, 2002).

In the last thirty years wireless communication technologies have seen a revolution. In the 1980s, wireless technologies were analogue signals (1Gb), in the 1990s they changed to digital (2Gb), it remained digital but became better quality and faster, and now the future is heading rapidly for 4Gb communications (Rob Flickenger, 2003). In 1994, the Ericsson telecommunications company began developing a technology named *Bluetooth*. After its initial development, Ericsson realized that the product had huge potential worldwide. Today's society demand to

see nature of today's society has seen technologies like *Bluetooth* and *Infrared* becoming an extremely popular alternative to wired communications and cables.

### 2.3 Definition of Wireless LANs

Most wireless LANs operates unlicensed frequencies at near-Ethernet speeds 10 Mbps, using carrier sense protocol to share a radio or infrared light medium. The majority of these devices are capable of transmitting information up to 1,000 feet between computers within open environment. In addition, most wireless LAN product offer Simple Network Management Protocol (SNMP) to support network management through the use of SNMP-based management platform and applications (Regis J. Bud Jr. , 2001). Figure 2.1 illustrates the concept of a wireless local area network interfacing with a wired network.



**Figure 2.1 :** A wireless local area network provides connectivity over the airwaves within a local area, such as building (Rob Flickenger, 2003)

The components of a wireless LAN consist of a wireless network interface card (NIC) and wireless local bridge, which is often referred as an access point. The wireless NIC will act as interfaces for to wireless network and the access point will connect the wireless network to wired network. Most wireless NIC interfacing to the wireless network by implementing a carrier sense protocol and modulating the data signal with a spreading sequence.



## 2.4 Definition of Network Monitoring

Network monitoring is the set of practice, technologies, and people that are deployed to measure and monitor the performance between communications and computer network and to suggest the corrective measures if a performance fault occurs or appears imminent (Jeffrey. *et al*, 2002).

The definition of network monitoring has changed over time. In the past, network monitoring meant monitoring a company's communication interfaces and receiving notification if the connection had broken down. A simple *ping* command, for instance, able to inform if any addressed network devices are not available. Naturally, network monitoring is used to help Administrator with pointing out a device that needs to be fixed. This solution might acceptable for organization. In the other hands, there is may unacceptable where uptime and performance requirements are tighter.

As monitoring system and practices evolved, network monitoring began to include more proactive performance measurement of computer hardware and communications technologies. Performance measurement system may monitor such things as CPU and disk utilization, server load, memory usage, router, firewall utilization and others. It might include polling of every pieces of equipment on the organization's network to determine the health of these components. Network monitoring system may even measure the response time of transactions and applications that are critical to the company or its bandwidth utilization. Measurements that fall outside of the boundaries of pre-set performance benchmarks can trigger an alert to monitoring personnel, or even an automated corrective response before the situation becomes serious and results in actual downtime. Such measurements can be stored in a database for proactive trend analysis and capacity planning.

## **2.5 Definition of Monitoring System**

In the computer definition, monitoring system is a system that used to sniff on the connection and gain some useful information about the connections. There are so many kinds of monitoring system such as network monitoring system, hardware monitoring system, memory usage monitoring system and others (Jeffrey. *et al*, 2002).

This monitoring system can be used to monitor the usage of the monitored things and get the statistic with collects the information requested by the users and displays it to the users or kept it in the log. This information from the monitoring system is used for data information collection or something else.

## **2.6 Monitoring Tools Function**

Monitoring systems are needed nowadays because of the increasing user in the internetworking. With this situation, network become heavy traffic places where there are lots of packets are being transmitted. On this traffic, information about how the usage of the wireless network will be gather for further action.

## **2.7 Capturing 802.11 Traffic**

Like LAN monitoring system, wireless monitoring are based on packet capture engines that listen passively for passing traffic. To observe radio networks at a fairly low level. Wireless monitoring system operate in scan mode, stepping through all or designated channels in a given band, dwelling on each for a short time. In addition, wireless monitoring offer capture filters to narrow a capture scope. For example, recording only packets associated with a given source, destination, or protocol. Some also use configurable triggers to observe packets until a specified pattern is detected, then start recording captured packets (Rob Flickenger, 2003).

## 2.8 Monitoring 802.11 Traffic

Wireless LAN technology standard 802.11 has the strongest momentum to becoming the main standard for corporate internal wireless LAN networks. The bandwidth of 802.11 is 11 Mbps and operates at 2.4 GHz Frequency. The 802.11 standard is designed to be faster speed and operate at a different frequency. Thus, captured traffic can be processed and presented in many ways, for example (Niall Mansfield, 2003):

- (a) Summarizing IP address activity in real time.
- (b) Decoding raw packet content into human-readable protocol fields and values.
- (c) Reconstructing TCP sessions or application dialogs.
- (d) Presenting tabular or graphed statistics regarding network usage.
- (e) Creating maps to visualize relationships and traffic flows between network nodes.

These features should be familiar to readers that have used traditional LAN monitoring. To provide these features, wireless monitoring must have a deep understanding of 802.11 protocols, security vulnerabilities, and potential performance problems. These are few of the many features offered by some monitoring system, either when operating solo or when used in conjunction with paired or third-party products. Thus wireless monitoring system given a quick taste of what monitoring tools can do. Wireless monitoring system varies considerably in terms of feature support, processing depth and breadth, presentation style, form factor, platform, and price (Niall Mansfield, 2003).

## **2.9 Analysis of Existing System**

Analysis on the existing systems are needed in order to determine what are the weakness in that systems. This analysis purposely to understand the usage and uses of the Wireless Monitoring System. The main activity in this phase are to understand the concept of the system, how it works, how it monitor the node, how it captured the packets and what is the software and hardware are needed to build the system. This analysis will become guidance in order to build another wireless monitoring system.

Next, the analysis is carry on with analyzing the existing system to find new ideas in order to upgrade the existing Wireless Monitoring System. Comparing between existing systems is done and the advantage and disadvantage on the existing system will able to use as an information to develop a better monitoring system than the existing system.

### **2.9.1 Current System Condition**

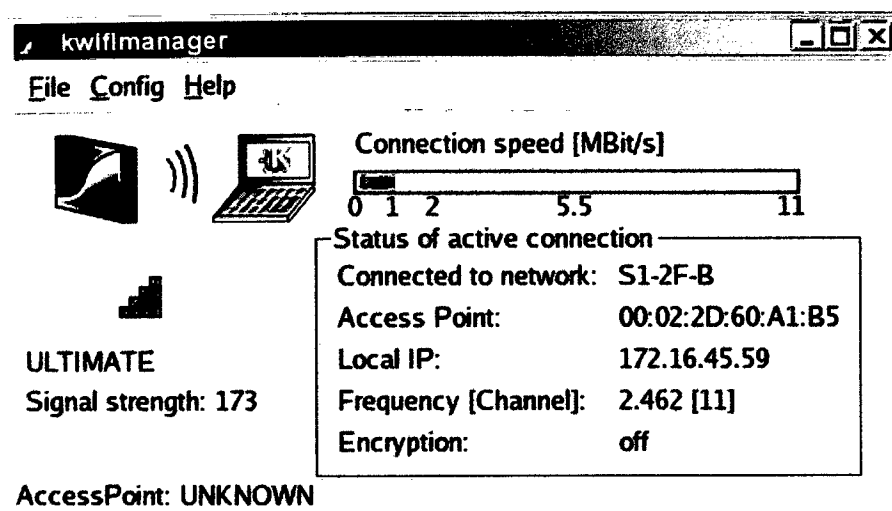
The system that had already been in market is not gives valid information about the packet that being capture in real time. Beside that, the graphical of existing system is not user friendly because it does not build using GUI. Existing system display the information in text based mode on the screen and not real time monitoring. The process of monitoring and capturing the information of packet are only available when the user requested by pressing key or typing a command. So that, the provided information might not be valid. Even some of the made system that had a GUI, but it only display the graph of the radio transmission wave strength and does not display the information about the packet that being capture.

Figure 2.2 and figure 2.3 show how Kwifimanager monitor the wireless signal. The system only monitor the signal wave from the wireless radio using four bars in green color as shows in figure 2.2. User would not know exactly total of data that being receive and transmit because it only show the strength of signal.



**Figure 2.2 :** Signal wave monitoring

Meanwhile figure 2.3 shows Kwifimanager that already exist in FEDORA. Eventhough this monitoring manager show the status of connection and the information of active connection but this application are not shows the rate of transmitting and receiving packets.



**Figure 2.3 :** Sample Kwifimanager that already exist in FEDORA

However, Kwifimanager are provide the graph that shown signal bandwidth as shown in figure 2.4, but this graph are not able to show the specific data and average data being receive and transmit through wireless network card.

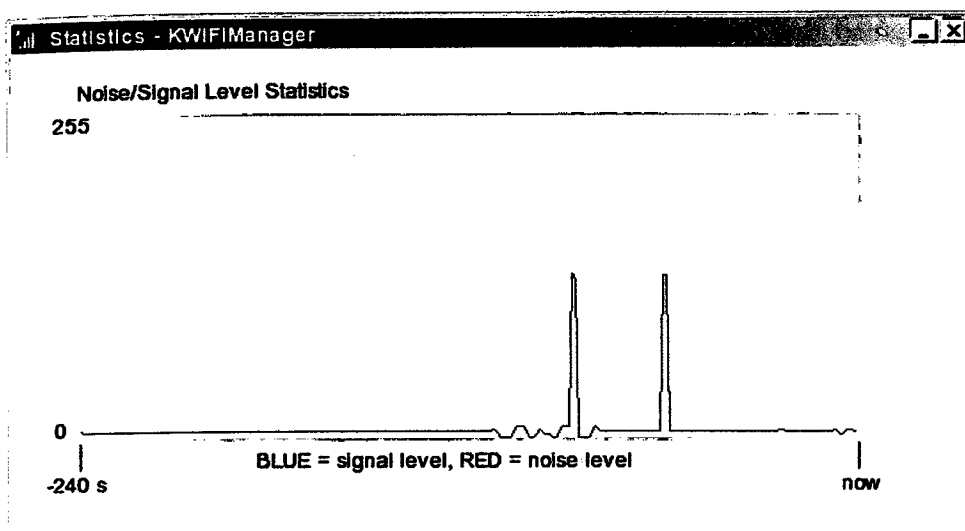


Figure 2.4 : Signal bandwidth monitor

Other existing system for wireless monitoring is using *ping* command. Figure 2.7 shows example of packet transmitting and receiving. *Ping* command use the text based to display information and it make harder to know exactly average of data being transfer and receive and error packet being capture. This method only able to use for monitoring single device only.

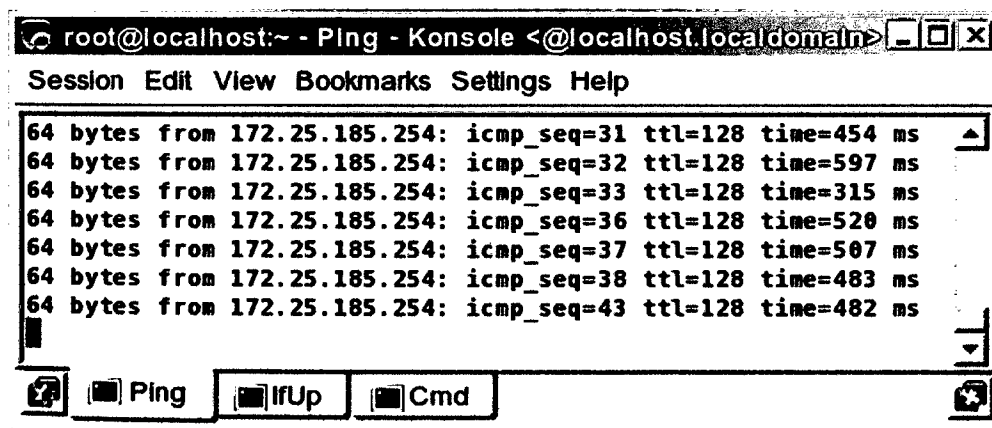
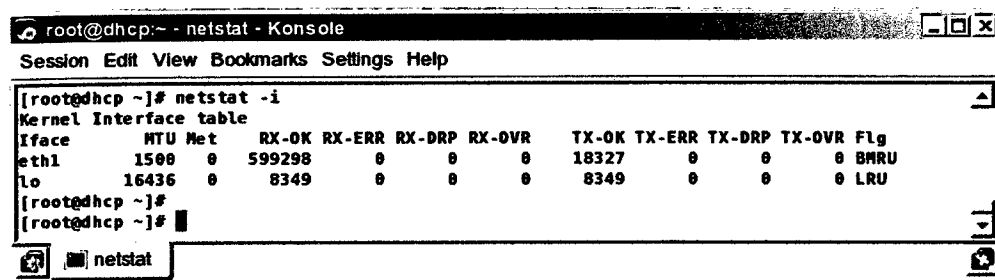


Figure 2.5 : Text based display information

Meanwhile *Netstat* command figure 2.8 shows example of packet transmitting and receiving, also error packet in transmission. *Netstat* command use the text based to

display information and it make harder to know exactly average of data being transfer and receive and error packet being capture. This method only able to use for monitoring single device only.



```

root@dhcp:~ - netstat - Konsole
Session Edit View Bookmarks Settings Help

[root@dhcp ~]# netstat -i
Kernel Interface table
Iface      MTU Met  RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth1       1500  0    599298      0      0      0    18327      0      0      0 BMRU
lo         16436  0     8349      0      0      0     8349      0      0      0 LRU
[root@dhcp ~]#
[root@dhcp ~]#

```

Figure 2.6 : Sample output using *Netstat*

## 2.9.2 Weakness for Current System

Through the analysis for monitoring system, Kwifimanager, *ping* command, and *Netstat*. There are several weakness identified. The weakness that identified are:

- (a) Kwifimanager monitor some information or only radio wave strength. It not specifically display amount of data or packet for easy narrative text rather than use graph to show the specific information.
- (b) *Netstat* only able to monitor the information that is needed at request time or capture the information at one time.
- (c) *Netstat* and *ping* command does not have GUI. It make harder to predict amount of data being send and transmit, more over when come to display average of packet that need to know.
- (d) *Netstat* and *ping* command only displaying the information in only text based that does not have real time in it, even though only in text based.

## 2.10 Proposed Solution

In order to create the wireless monitoring tools, so many problems arise when gathering the information. After gathering the information and making some analysis on the problem, these are the main problems arise and need to be overcome.

- (a) Having a specific node packet capturing. These capture the packets that are transmitted by the single node. If the monitored node is the specific one, it display the transmitted the packets information.
- (b) With the information that was display from the packet capturing, this generate a text based or graph on the usage of the bandwidth.

## 2.11 Selected Software for Development

In order to develop Wireless Monitoring System, several software are identified to use as a tools. *Ncurses* are selected as an interface for the system, meanwhile C language will be use to coding of engine. *GCC* will be use as a compiler for Wireless Monitoring System development phase.

### 2.11.1 Advantage Using *Ncurses*

*Ncurses* is library that able to provide programs to have a user friendly terminal based interface. *Ncurses* is a library that provides window functionality for text-based terminals. *Ncurses* is capable for:

- (a) Can use whole screen depend on the system want to be developed.
- (b) Use 8 different colors. It makes the display more colorful, rather than two colors in console which by default are black and white.