Remote Network Monitoring System (RNMS)

A thesis submitted to the College of Arts and Sciences in full Fulfillment of the requirement for the degree of Master of Science
University Utara Malaysia

By
Mohanad Naser Al-Hasanat

GRADUATE SCHOOL
UNIVERSITI UTARA MALAYSIA

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean of the Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to

Dean of Graduate School
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman.

Dedicated to my father Naser Al-Hasanat, my mother, my brothers,

my sisters, and to you my beloved wife …

ABSTRACT

Nowadays, computer networks become very complex. Thousands of nodes distributed in various places. Within this complexity, it has become impossible task to monitor large networks by human effort only. Thus, there are urgent needs to find convenient solutions to help networks managers in managing and monitoring their networks.

This study presents a monitoring system, named Remote Network Monitoring System (RNMS). The proposed system empowered the networks mangers to remotely monitor their network's computers. Therefore, a web-based monitoring system has been designed using UML models, and then the system has been developed using ASP.Net with VB.Net scripts. The proposed system is based on SNMP (Simple Network Management Protocol). The SNMP provides efficacious means to access the remote agent's MIB's (Management Information Base) objects. Furthermore, this study has evaluated and tested the RNMS using the verification test (unit, integration, and system testing), and the validation test (user acceptance test) based on TAM (Technology Acceptance Model).

ACKNOWLEDGEMENTS

First of all, I would like to thank Allah, for having made everything possible by giving me strength and courage to do this work.

Special thanks to my supervisor Mr. Amran Ahmad for his time, patience, and supporting during the development of this project, it has been an honor for me to work with him.

Finally, I would like to extend my thanks to my family and friends.

TABLE OF CONTENTS

CHAPTER FOUR: RNMS DESIGN

CHAPTER FIVE: RNMS EVALUATION

CHAPTER SIX:CONCLUSION

LIST OF TABLES

LIST OF FIGURES

Page

List of Abbreviations

RNMS	Remote Network Management System
SNMP	Simple Network Management Protocol
MIB	Management Information Base
MIB-II	Management Information Base II
FCAPS	Fault, Configuration, Accounting, Performance, and Security
NMS	Network Management Station
UUM	University Utara Malaysia
LAN	Local Area Network
WAN	wide Area Network
TCP/IP	Transmission Control Protocol/Internet Protocol
IETF	Internet Engineering Task Force
RMON	Remote Monitoring
RFC	Request for Comments
SNMPv1	Simple Network Management Protocol Version1
SNMPv2	Simple Network Management Protocol Version2
SNMPv3	Simple Network Management Protocol Version3
UDP	User Datagram Protocol
IP	Internet Protocol
OSI	Open System Interconnection
OID	Object Identifier
CPU	Central Processing Unit
MAC	Media Access Control address
UML	Unified Modeling Language
TAM	Technology Acceptance Model
PU	Preserved Usefulness
PEU	Preserved Ease of Use
SPSS	Statistical Package for the Social Sciences

CHAPTER ONE

INTRODUCTION

1.1 Introduction

This chapter provides a quick glance about the study; the background of the study, problem statement, objectives, expected contribution, scope of the study, research framework, and structure of thesis.

1.2 Background

In today's complex networked environments, where a network can range in size from a few nodes to thousands of nodes the way in how you monitor and manage your network devices is very important issue. This growing networks environment has to be managed in an effective way to derive the maximum benefit out of it. Network management comes for this reason it trades with controlling and monitoring the network devices in order to ensure its undisturbed and efficient operation.

Network monitoring provides the network's managers with information on the network status such as, the usage of a storage device. This information can be used to help the network manager to prevent abnormal situations like a hardware failure. The data then can be collected by polling the devices regularly or in some cases the devices themselves send alerts when some event occurs. On the other hand, network controlling can be done by changing the status of the controlled devices to perform specific events. In order to collect the data and to change the status of the network devices (Simple Network Management Protocol) SNMP protocol is used. SNMP provide a simple way to allow network manager to request values from the Management Information Base (MIB) in the managed device, and to set values in the MIB to affect the behavior of the managed devices (Raouf & Andreas, 2001)

ISO Network Management Model consists of five conceptual areas; Fault, Configuration, Accounting, Performance, and Security (FCAPS).

Prabhu S. & Venkat R. (2007) demonstrated each area of FCAPS as follow:

- **Fault management**: fault management aims to detect and notify network manager of any network problems to keep the network working effectively.

- **Configuration Management**: the goal of the configuration management is to monitor network devices to manage and track the various versions of hardware and software.

- **Accounting Management**: accounting management measures the network utilization parameters to regulate the uses on the network appropriately, and maximizes the fairness of the network uses across all users.

- **Performance management**: in this area the goal is to monitor the performance of the network devices so that the network performance can be maintained at an acceptable level.

- **Security Management**: the focus in this area is to control the access to network resources according appropriate authorization. A good example is to monitor and control the users logging in to the network resources.

However, this research will focus on monitoring the configuration, and the performance. This research proposes to develop a web-based monitoring system to allow network's managers to remotely monitor their network remotely anywhere and time.

1.3 Problem statement

Monitoring network devices is a very hard task especially when the numbers of the network's nodes are getting bigger. In University Utara Malaysia the computer labs supervisors still use the manual way to monitor their labs. They have to access each PC at once. They have to be there (physically). They spend a lot of time and effort getting information from each PC. The following table summarizes an interview with two of the computer labs administrators in University Utara Malaysia, Mr.Halim and Mr Zainol;

Table1.1: Mr.Halim and Mr.Zainol's Interview summarized

We have	Current situation
9 computer labs in the faculty of Information Technology	We use the manual way to access each PC in the nine labs in order to know what software is installed, the storage status, the devices status, and some other information
The average number of the PCs in each lab is about 35 PCs	
6 personalizes: 5 data entries and 1 technical	

There are many available network management systems (NMS) applications. It can be used to help the network administrators to manage and control their network devices remotely. However, Douglas and Schmidt (2001)

demonstrated that most of the network management applications are relatively expensive to purchase, setup, and to maintain. In addition, most of the recently major NMS software support only a few of popular versions of operating systems. Furthermore, the traditional NMSs do not support wide remote monitoring (i.e. web application).

In summary all above problems and limitations, UUM's computer labs administrators need a tool to allow them to remotely monitor all the computers inside their labs. This study proposes to develop a web-based NMS that allow the computer labs administrators to monitor any PC inside their labs anytime, anywhere.

1.4 Objectives

Following are the adjectives of this study:

- To design a web-based management system to monitor all the computers within a computer network.
- To develop a prototype of the proposed system
- To test and evaluate the prototype and its usability

1.5 Expected Contribution

The expected contributions of this study are:

- A working prototype of the Remoter Network Monitoring System (RNMS), which can be further enhanced and fully implemented in any Small and Medium Enterprises
- A general network monitoring model, which provides as good starting point when new SNMP based system is encountered.

1.6 Scope of the study

This study focuses on developing the RNMS system for the computer labs in University Utara Malaysia in particular.

1.7 Structure of Thesis

The chapters in this thesis are arranged as follows:

Chapter Two

Discuss the literature review which represents the previous related work to this thesis, and the existing works that have been conducted on the same area.

Chapter Three

Discuss the research methodology which will be adapted in this study. It discusses the steps in this methodology, and how they help the researcher to accomplish the study objectives.

Chapter Four

Will discuss the RNMS analysis and design process. It discusses the system that will be developed in a web based environment.

Chapter Five

Discuss the process of evaluate the proposed system. Two types of testing will be discussed; system validation test using TAM model and system verification test.

Chapter Six

The final chapter gives the conclusion of the study. Recommendations, directions of future work will be discussed, and concludes the findings of this research.

1.8 Summary

This chapter gives an insight of the proposed system by describing the background of the study, followed by the problem statement and the motivation factors that lead to the selection of the studied area. It also explains the objectives of conducting the study, as well as its contribution to the real world situation. The study scope also has been discussed in this chapter.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter presents a highlight on the literature review according to the area of the project. It gives an insight and reviews on the previous and existing works that have been conducted on the same area. This chapter is organized into three sections. The first section provides an overview and definitions of the network management systems and network management fundamentals. The second section will shed light on the Simple Network Management Protocol (SNMP), SNMP-based management models, Management Information Based (MIB), and SNMP basic operations. The last section will present the concept of three-tier architecture.

2.2 Network Management

The growing networks environment has to be managed in an effective way to derive the maximum benefit out of it. Since it is hard to manage this complex

infrastructure with human effort only, many Automatic Network Management tools come in response to this needs.

Clemm (2007) defined network management as:

"The activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems"

According to the previous definition, network management deals with four main areas;

- Operation; deals with keeping network and its services up and running smoothly by monitoring the network to detect the problems before the users affected
- Administration; deals with keeping tracks of all the network resources, and the how they assigned to the network
- Maintenance; deals with repairing and updating network resources
- Provisioning; deals with configure the network resources to provide a given service

Yongjun et al., (2008) define network management functions as “An effective network management system would promote network whole performance; ensure the normal operation of the services; grooming service traffic; exclude and restore network failure in time; improve network security and reliability, provide an effective, open, integrated and economic modern network for operators and users”

According to Lin & Wang (1999) network management systems used to maintain a network in a healthy operational condition, to monitor the status of the network, and to control the network to maximize its efficiency. Network management system is designed to view the entire network as unified structure, where each node is addressed and labeled and their attributes are known to the system. A feedback of status information is provided from each node to the network-control center.

As mention above, network management functions can be grouped into two categories; network monitoring “read function” which concerned with observing and analyzing the status and the behavior of the network resources and network controlling “write function” this concerned with changing the status of the managed devices and causing those components to perform specific actions.

A few reference management models have been implemented during the last three decades. The most widely used is the FCAPS (Fault, Configuration, Accounting, Performance, and Security) model, this model has been promoted by ISO (Flextoronics, 2005). The following section will elaborate more about FCAPS model.

2.2.1 FCAPS Model: The ABC of Network management

ISO Network Management Model consists of five conceptual areas; Fault, Configuration, Accounting, Performance, and Security (Prabhu S. & Venkat R., 2007). The following sections will introduce each of the FACPS functions categories in more details.

2.2.1.1 **F** is for **Fault**;

Al-Kasassbeh & Adda, (2009) defined fault management as "a set of functions performed to detect, isolate and correct malfunctions in a network. It also involves compensating for environmental changes, maintaining and examining error logs, accepting and acting on error detection, notifications, tracing, and identifying faults. Also fault deals with carrying out sequences of diagnostics

tests, correcting faults, reporting error conditions and localizing and tracing faults by examining and manipulating database information forms are part of the fault management functions"

Therefore, fault management deals with handling the faults that occur in the managed network, such as network's hardware or software failures. Fault management is therefore concerned with monitoring every device within network devices to ensure that it is working accurately. Also, fault management aims to ensure that network users do not affected by any network failure.

According to clemm (2007) Fault management can include:

- **Network monitoring and alarm management**; the first function of fault management is starting with network monitoring. Network monitoring allows network manager to see how the network operates -by keep track of the network status- and to visualize this status. Network monitoring also concerned with manage the fault alarms. Alarms can be defined as entreated messages sent from the managed devices in the network to notify the network manager about unexpected events. Alarm management includes two main functions:

1. Basic alarm management functions: include collecting alarms, maintaining accurate and current list of alarms, and visualizing alarms and network status.
2. Advance alarm management functions: functions to processing the alarms, functions acknowledge alarms (I see the alarm and I am handling it), and functions to clearing the alarms.

- Fault diagnosis and troubleshooting; the second function of the fault management is fault diagnosis and troubleshooting. The first step to solve a problem is to identify what caused it. The analysis process that leads to a diagnosis is referred to as root cause analysis. Figure2.1 illustrates a good example of how root cause analysis of "Device overheating" symptom lead to accurate repair action.

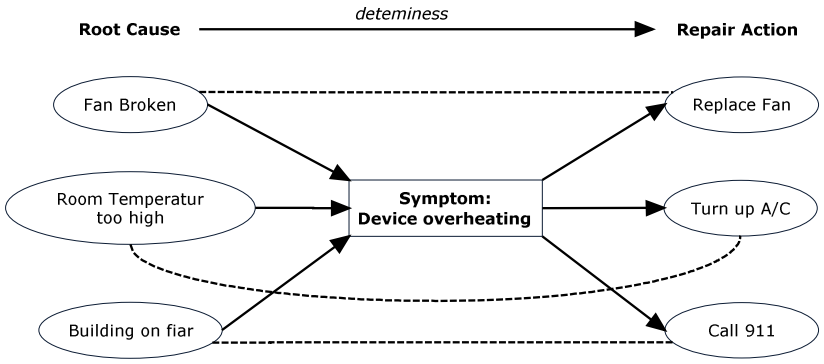


Figure2.1: Symptom, Root Cause, and Repair Action (Alexander Clemm, 2007)

Diagnosis the fault is supported by accurate troubleshooting. Troubleshooting tries to handle the root cause of the fault by retrieving additional information from the failed device (device that cause the alarm).

- **Maintaining historical alarm logs**
- **Trouble ticketing**; fault management deals with trouble ticketing. Trouble tickets are used to keep tracks of the resolutions of the network problems which require human intervention. Trouble tickets are issued by certain types of alarms or by customers when they experience a problem. Trouble tickets assigned to specific operator who is responsible for handling the problem.
- **Proactive fault management**; the last function of fault management is Proactive fault management. Proactive fault tries to predict the fault before it happened to avoid it.

2.2.1.2 C is for Configuration

Configuration management is concerned with the initialization, maintenance, and shutdown of network components (hardware or software). Configuration management is responsible for monitoring the configuration and making changes in response to user commands or in response to other network

management functions. Configuration management also may modify the configuration to bypass some fault within the network. Moreover, Configuration management involves the monitoring and controlling of convent normal operations in a network. Configuration management enables network's manager to generate, observe and modify operational parameters and conditions which govern the mode of operation of connections in the managed network. According to Kinga, & Huntb (2000) Configuration management deals with collecting information about hardware and software configuration. This information includes;

- Information about the devices in the managed network, their versions, locations, and their unique identifiers
- Capacity and location of the cabling in the managed network; the physical relationship between network devices

Clemm (2007) demonstrated configuration management functions as:

- Functions Configure managed resources; involves sending commands to the network's devices or services to change its configuration settings. For example; starting up a service, and shutting down a device.

- Auditing, discovery, and auto discovery; auditing means querying a network component (a device or a service) for configuration data to verify that the configuration of the network is what you expect it to be. On the other hand, discovery allows network's operators to discover what is inside the network.

- Synchronization management information; instead of auditing or discovering your network components it is more efficient to maintain a cache information about the entire network. Synchronization management insures that this information is an accurate reflection of the network. Three functions can be used to synchronize management information; Reconciliation, Re-provisioning, and Discrepancy.

- Backup and restore; includes functions to backup all the network resources. Backing up the network configurations is very critical issue in network management.

- Image management; includes functions to keep track of which software images are installed in which devices, have a way to deliver new images

to those devices when upgrade applied, and installing them without affecting their services.

2.2.1.3 A is for Accounting

Measuring the actual services provided and consumed is a critical part of network management. Audin & Lodge (2006) illustrated that; accounting management includes collecting information, preparing reports, analysis usage, invoicing, and cost of resource usage.

Accounting management functions can be categorized into two main aspects: costs for a communication medium and transmission functions, and costs for resources in the end systems. Here, the transmission system and the end system may belong to different accounting domain where every domain may have its own specifications of costs, and their own handling. Thus, there is a requirement to exchange cost information between each domain.

The following are some example of resources that could be subject to accounting management:

- Communication facilities: LAN, WAN, leased lines, dial-up lines
- Computer hardware: workstations, servers

- Software: application and utility software in servers, data base
- Services: includes all commercial communications and information services to network users

2.2.1.4 P is for Performance

An absolute requirement for the management of a network is the ability to measure the network's performance. Since you cannot manage and control a system unless you can monitor its performance. Collecting statistical data about the behavior of the managed objects and traffic flow between them can predicate the performance of those objects (Kinga, & Huntb, 2000). Therefore performance management functions try to maintain the entire network component at any acceptable level.

There are many types of indicators can be used to measure the network performance. The most popular are;

- **Availability**; the percentage of time that a network system, a component, or an application is available for users
- **Response time**; how long it take to respond to users requests
- **Accuracy**; what is the percentage of time that no fault is occur during transmission and delivering information

- **Throughput**; the rate at which application-oriented occurs
- **Utilization**; the percentage of the theoretical capacity of a resource that is being used

However, William Stallings (1993) argued that there are many problems facing the network managers to select appropriate indicators to measure the network's performance. Some problems are:

- There are too many indicator in use
- The meaning of most indicator is not yet clearly understood
- Some indicators are introduced and supported by certain manufactures
- Most indicators are not suitable for comparison with each other
- Frequently, most indicators are accurately measured but incorrectly interpreted
- For most indicators the calculation of indicators takes long time.

2.2.1.5 S is for Security

Finally, we come to the most critical area of network management; Security management. Management of security involves functions deal with protecting network components against any security threats and attacks. According to

Boutaba & Polyrakis, (2001) security management deals with security and safety in the networks. Security involves guarding networks components from active attacks. Where safety ensure the secure of exchange data through the network by preventing appropriate access to resources or data, eavesdropping, spoofing, and etc. also security management deals with user misconduct, as well as with protecting the network from unintentional damage or access to unauthorized resources.

Before examining the security management functions it is useful to characterize the security threats types first. Zhang et al. (2008) demonstrated the types of network threats as shown in tabel2.1:

Table 2.1: Security Threats and Assets

	Availability	Secrecy	Integrity
Hardware threats	Equipment is stolen or disabled, thus denying service	-	-
Software Threats	Programs are deleted, modified, thus denying access to user	An unauthorized copy of software is made	A working program is modified, either to cause it to fail during executing or to cause it to do some unintended task

Data Threats	Files are deleted, denying access to user	An unauthorized read of data is preformed. An analysis to statistical data reveals underlying data	Existing files are modified, or new files are fabricated
Communication Lines Threats	Messages are destroyed or deleted. Communication line are unavailable	Messages are read. The traffic pattern messages is observed	Messages are modified, delayed, reordered, duplicated, or fabricated

According to Douglas & Schmidt, (2001) there are three main groups of security management functions;

- **Maintaining security information**; this include functions to
    1. maintaining event logging
    2. monitoring security-audit trails
    3. monitoring usage and the users of security-related resources
    4. reporting security violations
    5. receiving notifications of security violations
    6. maintaining and examining security logs

7. maintaining backup copies for all part of the security-related files
8. maintaining general network user profiles, and usage profiles

- **Controlling resource access**: security management manages the access-control service by maintaining general network users profiles and usage profiles for specific resources (such as; security codes, routing table, and etc.) and by setting priorities for accessing those resources.
- **Controlling the encryption process**: security management must be able to encrypt any exchange between managers and agents. This function involves designating encryption algorithms and providing for key distribution.

2.3 SNMP (Simple Network Management Protocol)

The Simple Network Management Protocol (SNMP) is probably the best-known management protocol for managing networks (Douglas & Schmidt, 2001). It is widely used particularly in the data-network environment, and for monitoring applications. SNMPv1 is defined in a series of Internet Engineering

Task Force (IETF) in 1988. “The SNMP is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite” (SISCO Systems, 2009). Virtually all major venders of host computers, workstations, bridges, and routers offer basic SNMP. Work is even progressing on the use of SNMP over OSI and other non-TCP/IP protocol suites. Perhaps the most important of those initiatives is the development of a remote monitoring (RMON) capability for SNMP.

SNMP enables network managers to manage network performance, find and solve network problems, and plan for network growth. According to RFC 1157 Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements.

As SNMPv1 gained widespread support, it was a little too simple. Alexander clemm (2007) mentioned that SNMPv1 is notoriously inefficient at retrieving large amounts of management information. Moreover, it does support the concept of scoping or bulk requests, beside the minimal security it offers. This has resulted in SNMPv1 is being used mainly for monitoring, but not for controlling networks. For those reasons new version of SNMP was introduced; SNMPv2. The most important aspects of SNMPv2 as a protocol was the introduction of two new management functions: a get-bulk request (preserve repetition) and inform request (support reliability). Subsequently, a third version of SNMP was introduced SNMPv3 as respond to the weak points of the security issue in both SNMPv1 and SNMPv2.

2.3.1 SNMP-based Management Model Components

Zeng & Wang (2009); WANG et al. (2009) illustrated the elements of network management model that is used for SNMP. The model includes four elements; management station, management agent, Management Information Base (MIB), and network management protocol, as shown in figure2.2

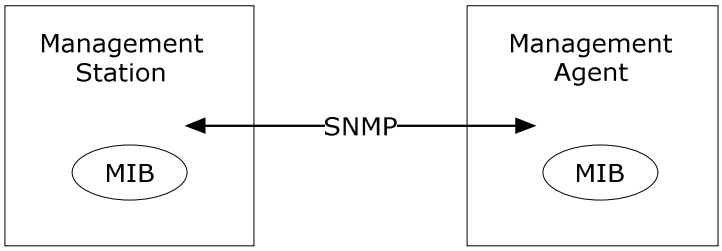


Figure 2.2: SNMP-Based Management Model (Wenxian Zeng & Yue Wang, 2009)

2.3.1.1 Management Station

Management station is the manger interface to the network management system. Management station has to have at minimum; a set of management applications for data analysis, fault recovery, an interface where a network manager can manage and monitor the network components, a protocol to provide the communication between management station and management agent, and a database of information about all the managed component within the network.

2.3.1.2 Management Agent

The second component is the management agents or management devices. RFC 1098 defined the management elements as devices such as

hosts, gateways, and the like, which have the management agents responsible for performing the network management's functions requested by the management station.

2.3.1.3 Network Management Protocol

The third component is the network management protocol. This component provides a simple communication between the agents and the network management applications. The SNMP can be layered atop several different transports and network stacks including the User Datagram Protocol (UPD) over the Internet Protocol (IP) as shown in figure 2.3.

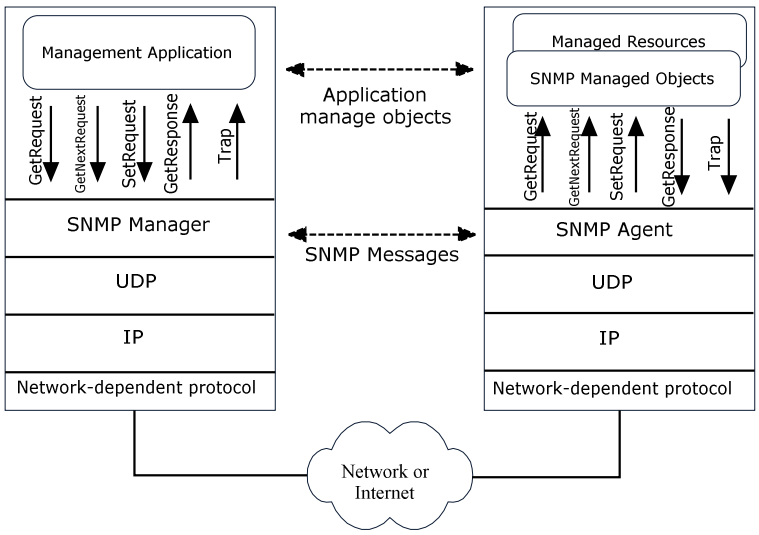


Figure 2.3: TCP/IP communication model and SNMP

(source: Amatzia Ben-Artzi et al., 1991)

2.3.1.4 Management Information Base (MIB)

As the way any network-management system, the foundation of a TCP/IP-based network management system is a database containing information about the elements to be managed. In both the TCP/IP and OSI (Open System Interconnection) environments, the database is referred to as Management Information Base (MIB) (Hatefi & Golshani, 1999). Each managed resource is represented by an object. The MIB is a structured collection of such objects. Wiesman et al. (2006) illustrated that; each node in the system will maintain an MIB that reflects the status of the managed resources at that node. A network management station can monitor the resources at any node by reading the value of its objects in the MIB. Also NMS may control the resources at that node by modifying those values. The MIB supports scalar integer types, strings, structures, and tables. The position of a data item in the tree is identified by a reference, called Object Identifier (OID). The OID is a sequence of numbers, usually denoted x.y.z.

Clemm (2007) illustrated four categories of management information;

- **State information**; includes the current state of the managed resources (logical and physical state), along with any operational

data. For example; current CPU loads, utilization of memory, and etc.

- **Physical configuration information**; includes information about the physical configuration of the managed device. For example, MAC address, serial number, and etc.

- **Logical configuration information**; includes information about the logical configuration of the managed device. For example, IP address, telephone numbers, and etc.

- **Historical information**; includes information about the performance-related state information, and logs of various types of events. For example, number if sent packets over the last day.

There are many MIB available to use. However, this study will use the MIB-II because it fulfills the requirements of the proposed system. The following section briefly describes this MIB.

2.3.1.4.1 MIB-II (Management Information Base –II)

As illustrated in the previous section, MIB is a collection of OIDs which represent the references of the managed object data in the agent side. MIB-II is adopted in this study because of its powerful features. Some of those features include:

- Provides new operational requirements
- Upgraded it is compatibility with SNMP
- Improved support for multi-protocol entities
- Improves the MIB readability and clarity by adding textual clean-up

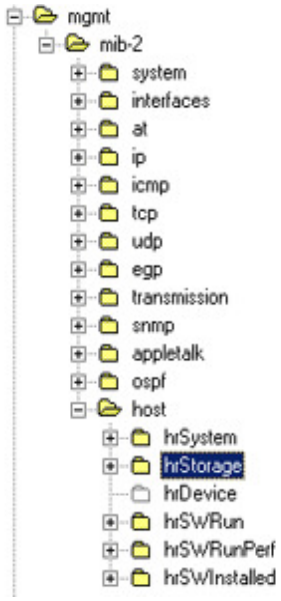


Figure 2.4: MIB-II Objects Groups

Figure2.4 shows the MIB-II Objects group. As shown above our concern in this study will be on the Host group. This group contains all the host

management OIDs. Start up from hrSystem, hrStoage, hrDevice, hrSWRun,hrWRunPerf, and ends up with hrWInsalled.

2.3.2 SNMP Basic Operations

SNMP provides a set of operations to access MIB's objects. The operations use OIDs (Object ID) to refer to the object in the MIB. Hatefi, (1999) and Wiesmann et al. (2006) illustrated the main management operations of SNMP as follow;

- **GetRequest**; network manager uses a GetRequest to retrieve information (MIB object) from an agent. The OID of a specific object is binding with the request. Also more than one MIB objects can be retrieved at a time.
- **GetNextRequest**; network manager uses a GetNextRequest to request management information from an agent. Unlike the GetRequest, here the OID in the binding request is not specified. Instead the agent is requested to return the object with the OID that comes next the last requested OIDs.
- **SetRequest**; network manager uses SetRequest to write in the agent's MIB (modify an object). The structure of the set request is

the same as GetRequest except that, in the case of SetRequest the object values in the variable bindings are not set to null, but contain the values to set the respective object to.

- **GetResponse**; an agent send GetResponse to a manger in response to a request. A GetResponse includes; the identifier of the request that contains the response to, an error status that amounts to a response code that indicate whether the request was successful or resulted error, an error index that carries further information in case of error, and a list of variable bindings.
- **Trap**; trap uses to convey an event by an agent to a manager. Traps include the information about who is emitting the trap, what occurred, when it was occurred, and additional information (conveyed in a set of variable bindings).

2.4 Three-tier Architecture

This project looks at the structural design of the solution as a three-tier model as depicted in Figure2.5. Each tier performs specific functions and uses different technologies.

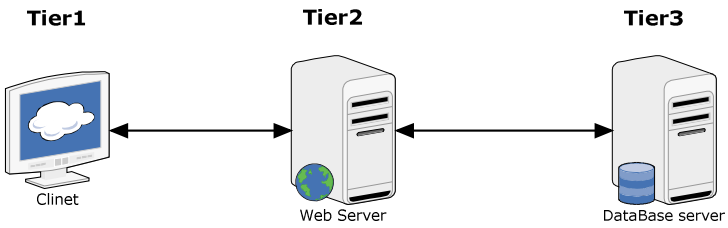


Figure2.5: Three Tiers Architecture

i) Tier 1: the first tier represents the user interface, navigation methods and tools. This is where the entire user experiences take place. This layer also provide graphic interface for users to interact with the application, input data, view results, manages data manipulation and formatting. In web applications, the browser performs tier 1 tasks.

ii) Tier 2: provides a link between the interface and the data service layer. This tier contains the business logic. Business logic govern application processing, connects the user with the data at the other end.

iii) Tier 3: represents the data services, provided by a data store, which manage the access to the application data.

According to Rong-Ceng and Zwe-Lee (2002); Fábio et. al. (2005) adopting the three tiers architecture has the following advantages;

- It is easy to modify or even replace any tier without effecting the system

- Adequate security policies can be enforced within the server tiers without hindering the clients
- It is support distributed computing which mean balancing load between network components

2.4 Chapter Summary

This chapter presents the concept of Network management. It elaborates more about the Fault, Accounting, Configuration, Performance, and Security (FACPS) model of network management. Also, this chapter describes the Simple Network Management Protocol (SNMP).

Moreover, this chapter elaborates more about the SNMP-based network management model components; Network Management Station (NMS), Managed Agent, SNMP Protocol, and the Management Information Base (MIB).

In addition, this chapter briefly describes the main SNMP operations; GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap. Also, this

chapter discussed the concept of the three-tier architecture.

CHAPTER THREE

METHODOLOGY

The previous chapter presented the literature review in the area of Remote Network Monitoring. This chapter will discuss the methodology that will be followed on fulfill the objectives of this study. Methodology is a sequence of systematic activities that are used as a guideline along the research in order to achieve its objectives. The purpose of having methodology is to simplify the analysis process and also to detail down the requirements and formulations of the study. This is important to ensure that the development, implementation, evaluation and improvement processes can be done smoothly. This chapter presents an overview about what methodology used to achieve the study objectives.

3.1 Introduction

According to Kuhn (1996); Lakatos (1978) research is an activity that contributes to the understanding of a phenomenon. All part of the phenomenon may be created as opposed to naturally opposing. Theoretically, phenomenon is a set of behaviour of some entity(ies) that is found interesting to the researcher. But in order to know the phenomenon, the researcher must first understand the knowledge that allows prediction of the behaviour of some parts of the phenomenon. Here, understanding and knowledge is the most important elements for the researcher, so the set of activities a research community considers appropriate to the production of understanding are its research methods or techniques.

As stated in the first chapter of this research, the objectives of the study are basically to design and develop a prototype for a Remote Network Management System (RNMS), and to evaluate it is usability. Thus, the project's operational framework will be adopted from the General Methodology of Design Research. The following sections will describe in more details the project operational framework.

3.2 RNMS Operational Framework

The framework of this study will be a modified framework of The General Methodology of Design Research proposed by (Vaishnavi & Kuechler, 2004). The proposed framework contains the major phases as shown in Figure 3.1.

- Awareness of Problem, and planning
- The Problem analysis
- Design
- Development
- Testing and Evaluation
- Finalize and document the System

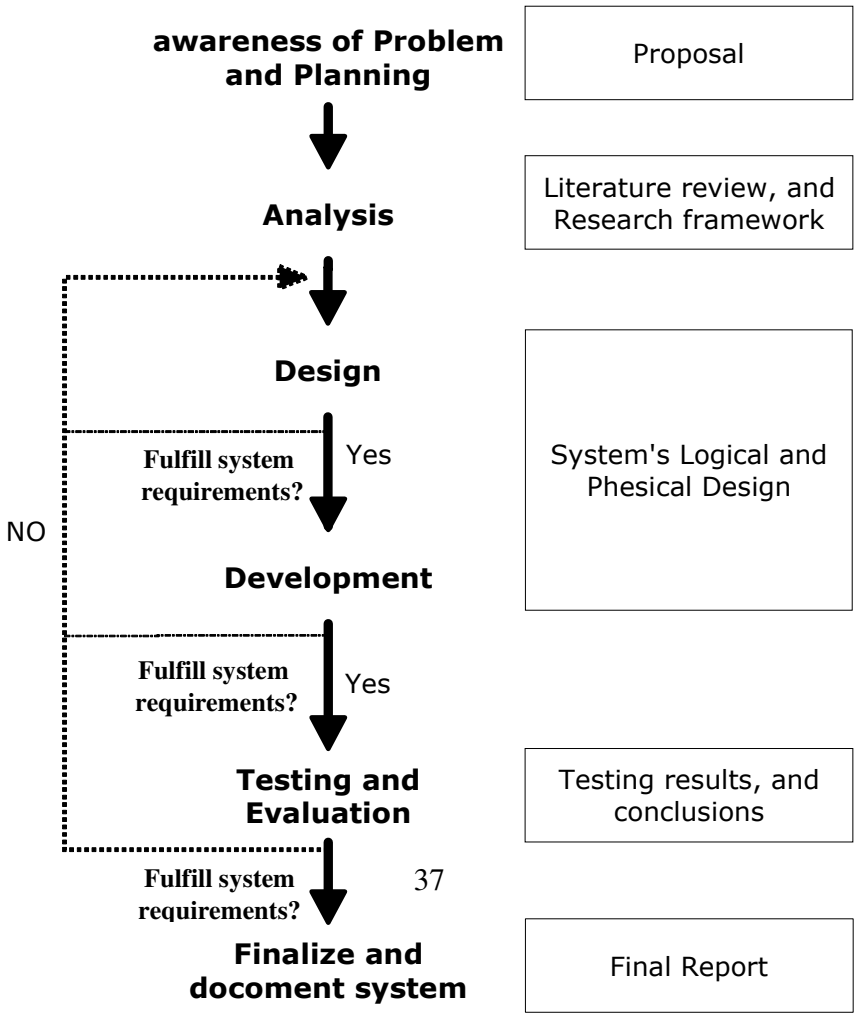


Figure 3.1: Project Operational Framework

3.2.1 Awareness of Problem and Planning

The primary objectives of this phase are to observe and identify the problem area. Based on the problem statement of this study; firstly the researcher is going to determine the problem and then elaborate the objectives and the scope of the study. The following are the activities that involve in the awareness phase:

- Define the problem background and problem statement
- Define project objectives
- Identify project scope and constraints

The awareness of the problem will be solved through interviews with the UUM computer lab supervisors. In this stage also, the researcher will put the

project schedule. Thus, the output of this phase will be chapter 1 of this research.

3.2.2 Problem Analysis

Problem analysis phase involves decomposition the whole system by taking a complex problem with complicated information requirements and breaking it into smaller and more understandable components. The purpose of the analysis phase is to understand the problem background and to determine the research methodology. The primary activities in the analysis phase are; gathering literature review, and define system framework.

3.2.2.1 Review literatures

This phase involves deeply understand the study problem, and the past researches that have been done in the same area. Literature review is done by gathering and referring information from general, primary and secondary sources. Firstly, the general sources provide an overview of a topic and provide lead to where information can be found such as Internet and weekly magazine news. Secondly, the secondary sources are review papers and textbook to understand the research basic

concept that will develop further understanding on the project. Finally, the most important sources are the primary sources. These are accounts of the actual researches that have been done. It appears as journal articles or other originals work including abstract.

3.2.2.2 Define the Framework

This phase involves constructing the study framework. Thus, the researcher will examine several candidates of common methodologies to verify the study framework. As illustrated in previous sections the study framework was inspired from the General Methodology of Design Research. The researcher created and adopted his own framework as shown in figure3.1

3.2.3 Design Phase

In this phase system architecture, system requirements, hardware and software that will be used for this project will be determined. Following are the details;

3.2.3.1 System Architecture

The architecture of the proposed system will be modeled as a Three-tier models as demonstrated in the second chapter of this the thesis. Figure3.2 shows the proposed system architecture in more details;

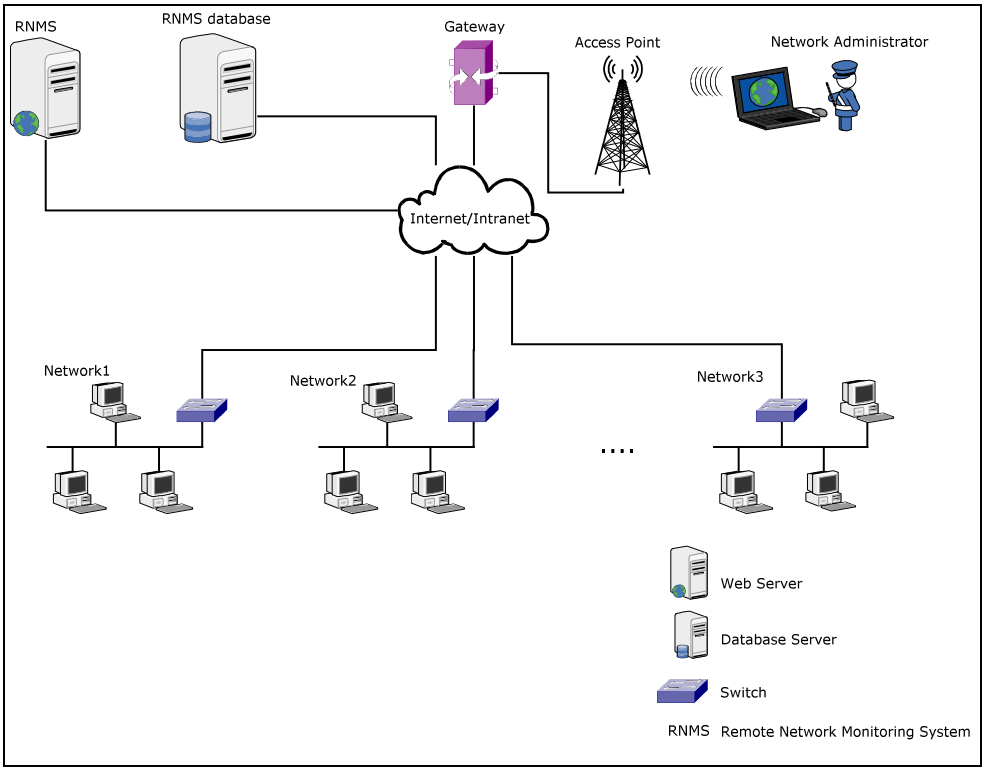


Figure3.2: The proposed RNMS architecture

As shown in the previous figure the network administrator use any PC with internet connection and browser to connect to the RNMS system located in the web server. The administrator can use the RNMS interface to access all the RNMS functions. The administrator can archive all the retrieved information from the monitored PC to the RNMS database.

3.2.3.2 System requirement design

In this phase, the system requirements will be defined. For the purpose for this project, the object oriented approaches that will be used is Unified Modeling Language (UML). Four types of diagrams will be used to define the application requirements in order to develop RNMS during this phase:

i. Class Diagram
ii. Use Case Diagram
iii. Activity Diagrams
iv. Sequence Diagrams

These diagrams will be presented in chapter four. In this phase also the researcher will design:

i) The user interfaces
ii) Database; this includes define tables and the relations among those tables.

3.2.3.3 Hardware specification

Basically, a personal computer with operating system can be used to develop and employ the proposed system. However, better hardware specifications will enhance the system performance especially on the server side.

The specifications of hardware that has been used to develop the RNMS is described in the following table:

Table3.1: Hardware Development Specification

Hardware	Specification
Processor	Genuine Intel(R) CPU T2250 @1.73GHz (2 CPU)
Memory	2 GB DDRAM
Hard disk	120 GB
Monitor	15"
Input and output devices	Keyboard and Mouse
Network Interface Card	Intel(R) PRO/100 VE Network Connection

3.2.3.4 Software Specifications

Software will play important roles in developing the proposed system and preparing the report for this study. The software specifications used for developing the RNMS are;

- Windows XP Professional SP3
- SNMPV
- MIB-II
- Visual Studio .NET 2005
- MSSQL 2005
- Adobe Photoshop CS2
- Smart Draw 2007

3.2.4 Implementation Phase

A prototype system will be developed based on the analysis and design phases. This phase basically involves programming and coding of the system. At the end of this phase, the overall architecture of the system is developed. All the activities are achieved by referring to the object-oriented methodology such as class diagram, use case diagram, activity diagram and sequence diagram.

The evolutionary prototyping methodology is the normal technique used for web-site development and large project with many users

(Knight,Steinbach,and Kellen, 2001). The prototyping approach process contains four main steps which adapted from (Naumann and Jenkins, 1982), as shown in figure3.3.

Gordon and Bieman (1995) illustrated the benefits of using prototyping as:

- Improved system usability.
- A closer match of the system to users' needs.
- Improved design quality.
- Improved maintainability.
- Reduced development effort.

The process of prototyping involves the following sections.

3.2.4.1 Identify the problem

Based on the requirements that have been identified in the design phase, the prototype will be started with the first requirement then and go on to the next step.

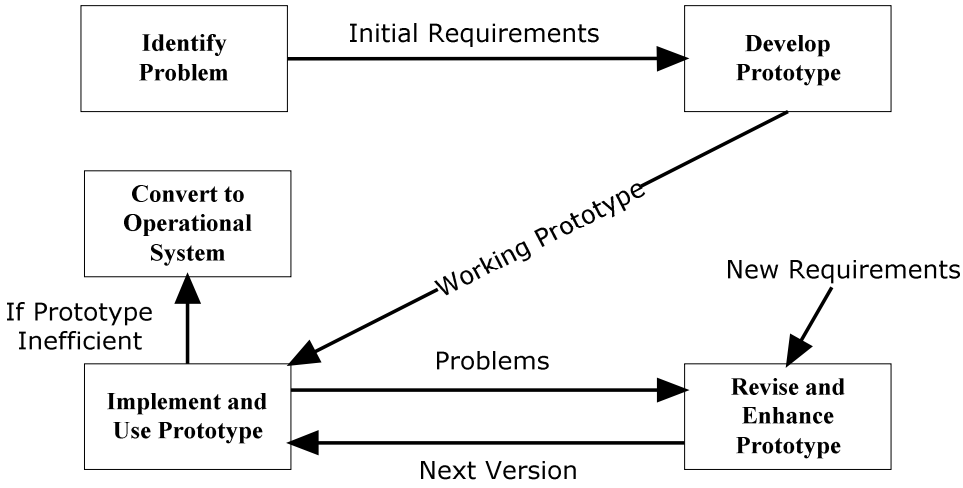


Figure 3.3: The prototyping approach (Naumann and Jenkins,1982)

3.2.4.2 Develop initial Prototype

Prototyping is the process of putting together a working model in order to test various aspects of the design, illustrate ideas or features, and gather early user feedback. The purpose of prototyping is to eliminate the possibilities of uncertainty and misunderstanding, and to verify a solution at an early stage of design.

This phase basically involves programming and coding of the system .The initial prototype is developed by including programming (coding). This study used ASP.Net embedded with VB.Net as a programming language to develop the prototype. At the end of this phase, the overall

architecture of the system will be developed. All the activities are achieved by referring to the object-oriented methodology such as class diagram, use case diagram, and sequence diagram. Essentially, a prototype enables the developer to fully understand how easy or difficult it will be to implement some of the features of the system. It can give users a chance to comment on the usability and usefulness of the user interface design, and to access the fit between the software tools selected the functional specification and the user needs.

Prototypes can be categorized in various ways. According to Bahrami (2000), there are four commonly accepted prototypes. There are:

i) **Horizontal Prototype**

Horizontal Prototype is a simulation of the interface but contains no functionality. The advantages are very quick to implement, providing a good overall feel of the system, and allowing users to evaluate the interface on the basis of their normal, expected perception of the system.

ii) **Vertical Prototype**

Vertical Prototype is a subset of the system features with complete functionality. The principal advantage of this method is that few implemented functions can be tested in great depth. In practice, prototypes are hybrid between horizontal and vertical. The major features of the interface are established so the user can get the feel of the system

iii) Analysis Prototype

Analysis Prototype is an aid for exploring the problem domain. This class of prototype is used to inform the user and demonstrate the proof of a concept. It is not used as the basis of development, however, and is discarded when it has served its purpose. The final product will use the concepts exposed by the prototype, not its code.

iv) Domain Prototype

Domain Prototype is an aid for the incremental development of the ultimate software solution. It often used as a tool for the

staged delivery of subsystems to the users or other members of the development team. It demonstrates the feasibility of the implementation and eventually will evolve into a deliverable product.

For the purpose of this project, the horizontal and vertical prototype will be used. The prototype will be conducted for several times until the end user satisfied. Users can generally provide better feedback about requirements when examining prototype.

3.2.4.2.1 Implement and use prototype

The UUM Computer lab supervisors and UUM IT students will examine the prototype. Once prototype is accepted, the development of final system will begin. The additional implementation will be added into the system based on prototyping.

3.2.4.2.2 Reverse and enhance the Prototype

After using the initial prototype by the users, the new requirements have to be rebuilt and enhancement the prototype based on the users' feedback.

3.2.4.5 Build the final system

Once prototype is accepted, the development of final system will begin. The additional implementation will be added onto the system based on prototyping.

3.2.5 Testing and Evaluation

Testing and user acceptance test will be conducted after develop the final system. Following are the details;

3.2.5.1 Verification Test

This phase involve test the proposed system to ensure that the system fulfils the user requirements. For the purpose of the project unit,

integration, and system testing will be implemented. Black box strategy will be used for integration testing (since the system functionality is the main concerned but not the way how the system is implemented).

3.2.5.2 Validation Test

In this phase user satisfaction test will be implemented based on Technology Acceptance Model (TAM) to ensure that the system will be accepted among the users. According to Bahrami (2000), user satisfaction test or user acceptance test is the processes of quantifying the usability test with some measurable attributes of the test. Chapter five will discuss more about the user acceptance test.

3.2.6 Finalizing and Document the System

Report writing is the last part of the study which includes the documentation of the system. In the report, the details of the discussion as well as its finding will be presented.

3.3 Summary

This chapter present the methodology of the study, which describes the project framework. The framework of this study is inspired from the General Methodology of Design Research -Proposed by Vaishnavi & Kuechler (2004) –. Six mains phases were discussed in this chapter; awareness of problem and planning, problem analysis, design, development, testing and evaluation, and finalize and document the system.

CHAPTER FOUR

RNMS DESIGN

4.1 Introduction

In order to develop a useful computer application, you have to design a good model before start coding a single line. “Even in the case of a single developer working alone, it is still advisable to construct visible models. Software development is a complex activity and it is extremely difficult to carry all the necessary details in one person’s memory” (Simon B. et al., 2006). This chapter will cover designing and implementing RNMS; system requirements (using UML diagrams), system architecture, and RNMS’s interfaces design.

4.2 RNMS requirements

According to Dennis et al. (2005) identifying the requirements for any application supports the development and the implementation steps. Sections 4.2, 4.3 will describe the functional requirements and the non-functional

requirement of the RNMS. In the priority column, the following short hands are used:

- M – mandatory requirements (something the system must do)
- D – desirable requirements (something the system preferably should do)
- O – optional requirements (something the system may do)

4.2.1 RNMS Functional Requirements

Following are the main functional requirements:

Table4.1: RNMS Functional Requirements

No.	Requirement ID	Requirement Description	Priority
	RNMS_01	**View Current PCs' Details**	
1.	RNMS_01_01	View General Information	M
2.	RNMS_01_02	View Storage Information	M
3.	RNMS_01_03	View Running Processes Information	M
4.	RNMS_01_04	View Installed Software Information	M
5.	RNMS_01_05	View Devices Information	M
6.	RNMS_01_06	View CPU Load	D
7.	RNMS_01_07	View Managed PCs' Details Charts	D

8.	RNMS_01_08	View Managed PCs' Details Reports	D
	RNMS_02	**Handling Computers List**	
9.	RNMS_02_01	Add New Computer	M
10.	RNMS_02_02	Remove Computer	M
	RNMS_03	**Managed Administrator Account**	
11.	RNMS_03_01	Change Password	M
12.	RNMS_03_02	Change Email	M
13.	RNMS_03_03	Password Recovery	D
14.	RNMS_04	Login	M
15.	RNMS_05	Logout	M
16.	RNMS_06	Connect to PC	
	RNMS_07	**Generate Archives**	
17.	RNMS_07_01	Archive General Information	M
18.	RNMS_07_02	Archive Storage Information	M
19.	RNMS_07_03	Archive Running Processes Information	M

20.	RNMS_07_04	Archive Software Information	M
21.	RNMS_07_05	Archive Devices Information	M
22.	RNMS_07_06	Archive CPU Load Information	M
23.	RNMS_07_07	Archive Charts	D
24.	RNMS_07_08	Archive Reports	D

4.2.2 RNMS Non Functional Requirements

Table4.2 lists the RNMS non-Functional requirements;

Table4.2: RNMS Non Functional Requirements

No.	Requirement ID	Requirement Description	Priority
	RNMS_08	**Reliability issues**	
24.	RNMS_08_01	• The system should provide a feedback about crashes. • The system should be up-to-date with its contents. • The systems should behave perfectly when reloaded again after a crash.	M
	RNMS_09	**Usability issues**	
25.	WBRS_09_01	System should be user-friendly; simple and clear navigation system, provide	M

		custom error pages, and content should be clear and simple	
	RNMS_10	**Security Issues**	
26.	WBRS_10_01	The system should provide a secure login page and enable user to change his/her password.	M

4.2.3 RNMS USE CASE Diagram

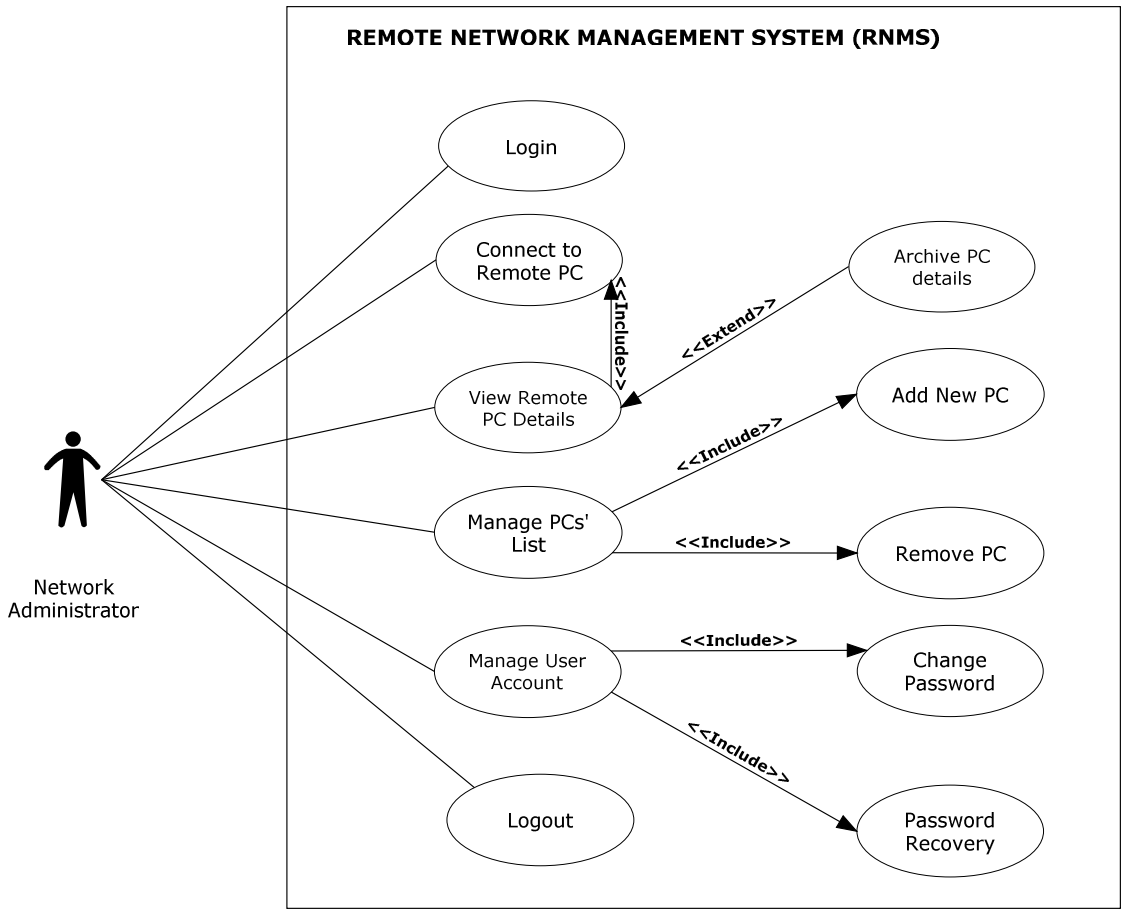


Figure4.1: RNMS USE CASE Diagram

4.2.4 USE CASE Specifications

Following are the RNMS USE CASEs specifications. USE CASEs specifications arranged according to the requirements list table.

4.2.4.1 USE CASE: View General PC Information (RNMS_01_01)

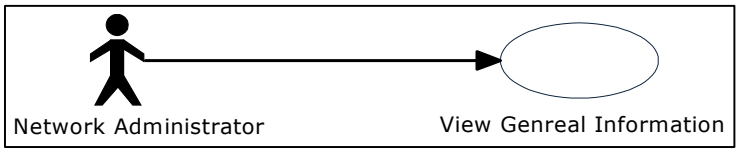


Figure4.2: View General PC Information

BRIEF DESCRIPTION

This use case is initiated by the network administrator. This use cannot be initiated unless the administrator has a successful login to the system. This use case enable network administrator to view general information about the monitored PC, Computer Name, Operating system and Hardware brief description, administrator contact, PC location (taken from windows), system stating up time, system current date and time, number of running processes, and number of windows user.

PRE-CONDITIONS

The Administrator must be login successfully to the system, and the system has a successfully connect to the selected PC.

CHARACTERISTIC OF ACTIVATION

Event driven (Administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the administrator presses on the "General Information" navigation button in the home page main menu.
- If the system successfully connects to the remote PC (using the IP chosen by the user) the system shall display General Information about the connected PC on the screen.
- The administrator can view updated information about the remote PC by press the "Refresh" button to re-connect again with the remote PC and get it is current status.
- The administrator can press "Save to Archive" button to initiate the **Archive General Information USE CASE (RNMS_07_01).**
- If the system could not connect to the remote PC then the system shall display a message to inform the administrator about what error was happened. (Exception follow **E1)**

Alternative Flow

Not Applicable.

Exceptional Flow

E-1: Connection Error (RNMS_01_01_01)

The system shall display a message about what error was happened while trying to connect to the remote PC. The system shall not show the "**Save to Archive**" button.

E-2: Web Server Error (RNMS_01_01_02)

If the server is crash then the system shall display "**The Server is Down**" button.

POST-CONDITIONS

- The administrator will be able to archive what information the system is display about the remote PC.

RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable.

The complete USE CASE specifications are attached at Appendix C page 100.

4.2.5 Activity Diagrams

The compete activity diagrams are attached at Appendix A page 87.

Following is the activity diagram of view PC details;

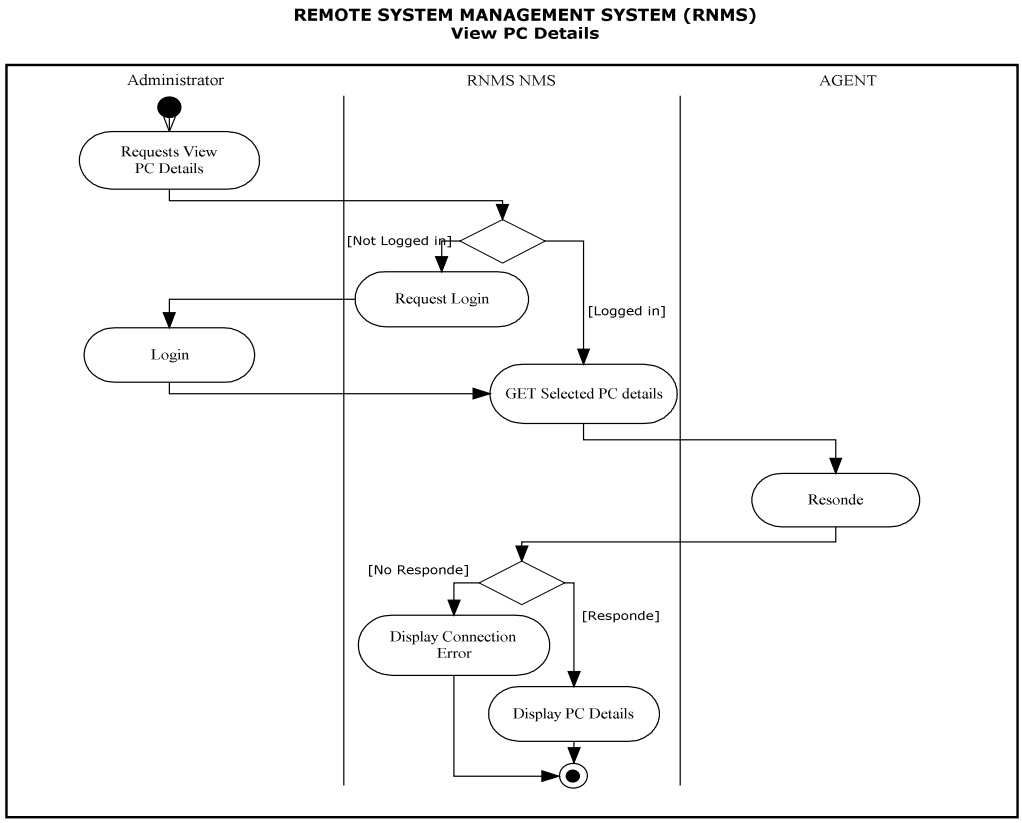


Figure4.3: View PC details activity diagram

4.2.6 RNMS Sequence Diagrams

The compete activity diagrams are attached at appendix B page 95.

Following is the sequence diagram of view PC details;

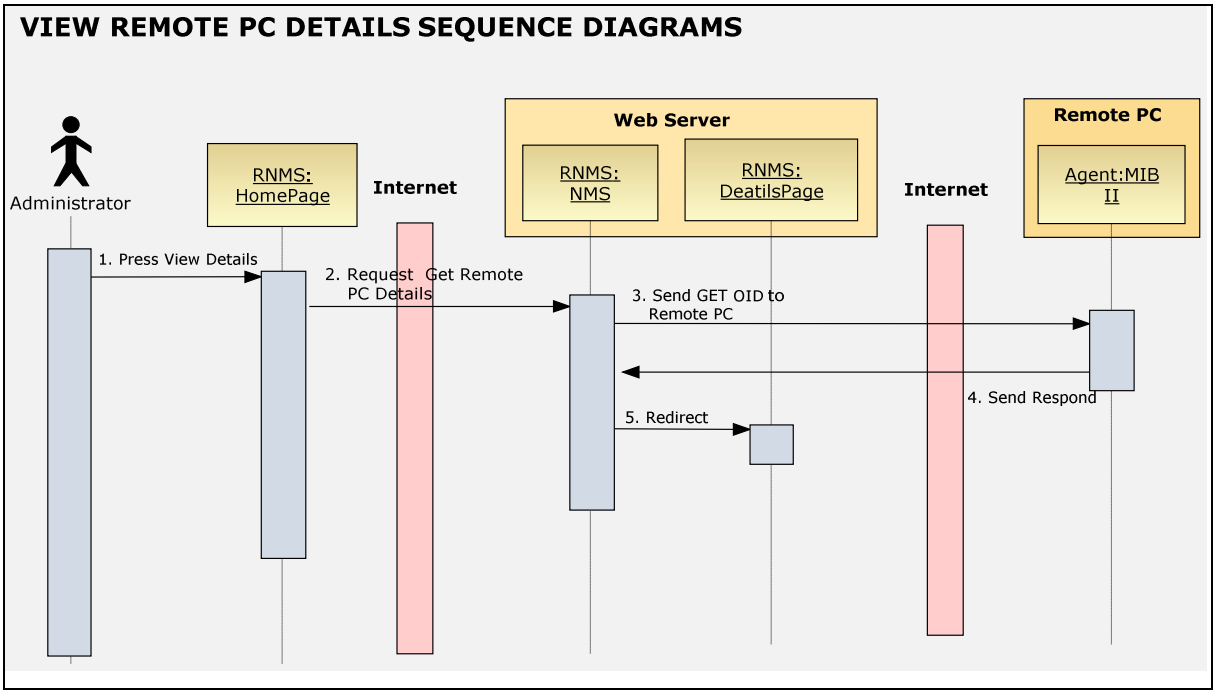


Figure 4.4: View PC details Sequence diagram

4.2.7 RNMS Class Diagram

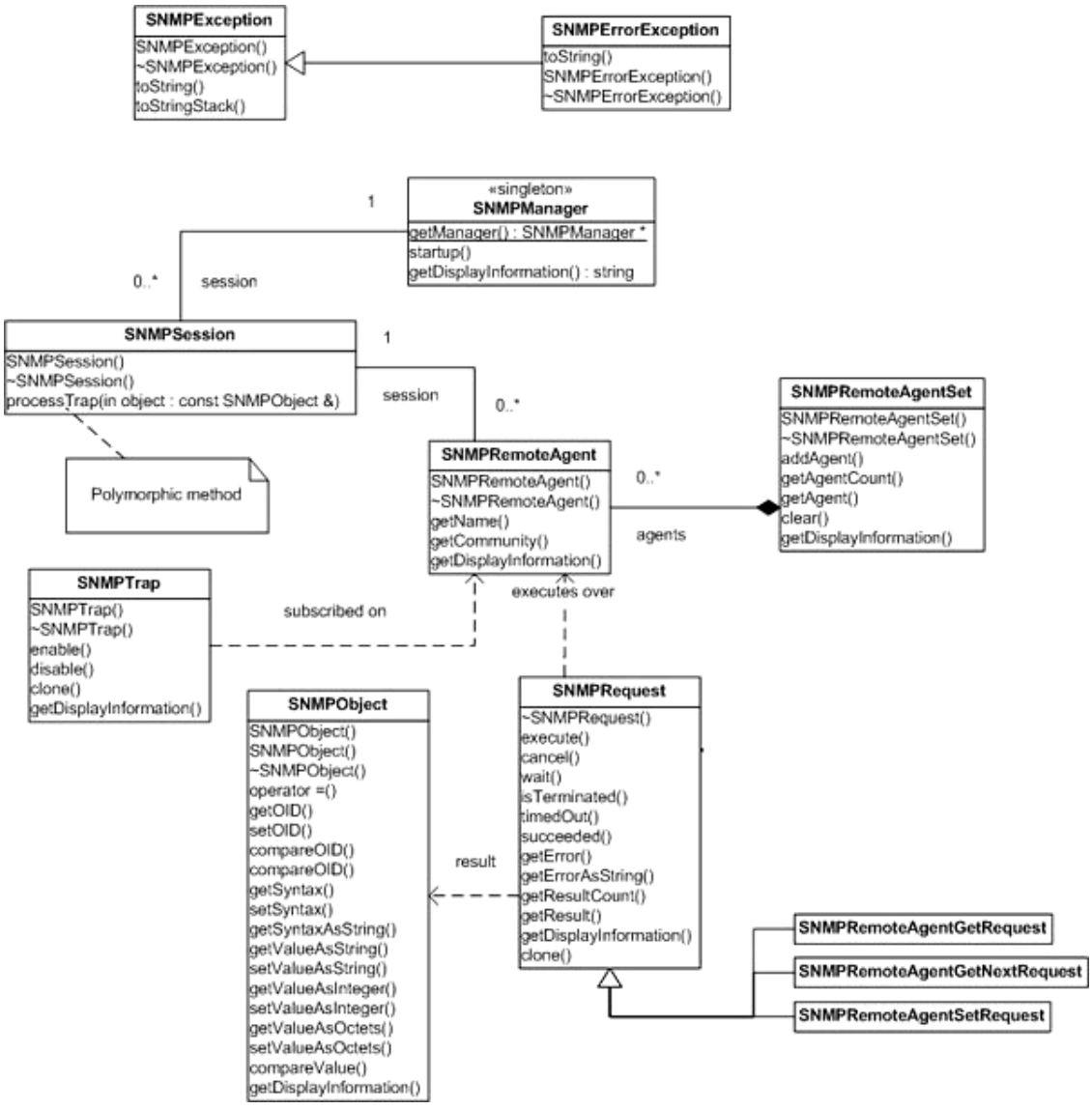


Figure 4.5: RNMS Class Diagram

4.2.8 RNMS Interfaces

After modeling the RNMS system using UML diagrams, the prototyping process will start. Figure4.6 shows the RNMS Home Page.

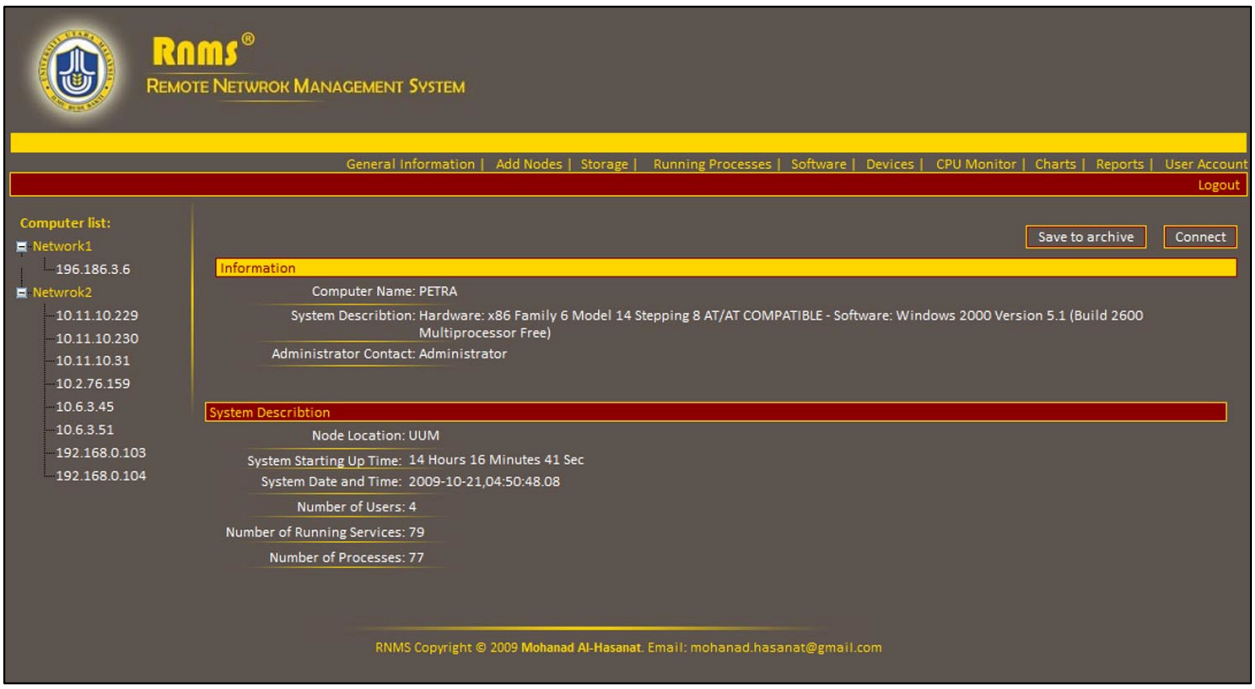


Figure4.6: RNMS Home Page

The complete pages design is attached at Appendix D page 152.

4.3 SUMMARY

This chapter discussed the findings of the research. It illustrated the system design process using UML diagrams. System requirements have been conducted. Use case diagrams, activity diagrams, sequence diagrams, and class diagrams have been sketched. Also, RNMS pages have been designed.

CHAPTER FIVE

RNMS EVALUATION

5.1 Introduction

Referring back to the third objective of this study - To test and evaluate the RNMS prototype and its usability - This chapter will discuss the process of evaluating the proposed system. This chapter is divided into two main sections; verification testing section and validation testing section. The verification test section is divided into three subsections; unit test, integration test, and system test subsection. While the validation test will discuss the user acceptance test.

5.2 RNMS Verification Test

According to Dmitry at el. (2009); Pierce (1995); Doron at el. (2005) verification test is a quality assurance test aims to make sure that the system accomplish its desired requirements. Its tries to answer the question “Have you built the system right?". There are two approaches to perform the verification

test; dynamic test and static test. Static verification test is done by physically examine the system. For example; code convention test. During the implementation phase of the proposed system this test is done for all the system's functions.

On the other hand, the dynamic verification test or sometime called experimental test is performed during the execution of the application to check its behavior in some circumstances. Dynamic test can be categorized - according to the scope of the test- into three main phases; Unit test (a single function or class), integration test (more than one unit), and system test (test the whole system). In order to evaluate the verification of the proposed system, the system was subjected to these three testing phases. The details will be described in the following sections.

5.2.1 RNMS Unit test

A unit is a smallest atomic testable part of a developed application source code (Beydeda S., 2005; Bin Xu, 2009). It could be a function, procedure, or even a class or a method. In this phase the programmer will examine each unit of the source code versus it specification simply

by taking each unit, isolate it, and test whether it behave like what we expect (Board I. S, 1986)

For the purpose of the proposed system, the source code was divided into 34 separated units. Each unit was tested individually. The debugging results were noted. Some errors corrections were made for some units to maximize its performance and to correct its functionality.

5.2.2 RNMS Integration Test

Integration test is performed after the unit testing and before system testing (Ma Liangli et al., 2007). Integration test involves testing combined units (units must have been passed the unit testing) together into modules. Ursula & Monika (1990) illustrated that Integration test takes a module as it is input, verify it is performance, functionality, and reliability by exercised their interfaces using any types of integration tests (Black Box, Bin Bang, and etc.) and delivered as it output "the integrated system is ready for system testing".

In this stage the RNMS's main USE CASEs will be tested using the Black Box technique. According to Tafline and Karl (2001); Harrine (2002) black box (also known as close box) is a test derived primarily

from a programmer's specification. The internal source code is not considered at all (i.e. treat the system as a black/closed box). Black box test tries to exercises all the system functional requirements before the software is ready for production. Table5.1 shows the results of RNMS's black box testing.

Table 5.1: RNMS Black Box testing (integration test)

ID	Module	Verification	Expected Result	Actual Result
1	Login	Enter a valid username and Password	Redirect the user to the main page	valid
		Enter invalid username and valid password	Request the login again	valid
		Enter valid username and invalid password	Request the login again	Valid
		Blank username or password	Show required field message	Valid
2	Connect to Remote PC	SNMP Service is not running	Show "No respond" message	Valid
3	View Remote PC Current Details	Change the remote PC current state (for example; attached new storage device)	View the current PC details including the new storage device details	Valid
		Shutdown a process on the	View the current	Valid

		remote PC	processes status excluding the terminated process	
		Add/Remove new Software	View the latest Software list including/excluding the Added/Removed software	Valid
4	Add New Node	Entered a valid IP address format	Show “Incorrect IP address Format” message, and don’t add the node	Valid
		Enter existing IP address	Show “This node is already add” message, and don’t add the node	Valid
5	Remove Node	Select any node from the PC list, and press REMOVE button	Remove the selected IP Node, and show “The selected node has been successfully removed” message	Valid
6	Change Administrator Password	Entered invalid administrator password in the “current password” textbox	Request the current password again	Valid
		The entered new password is	Show a weak password	Valid

		too short (less than 6 digits)	message, and don't change the password	
		The entered new password and the confirmed password did not match	Show password not confirmed correctly	Valid
		Enter a correct data (valid current password, new password, confirm the new password)	Show "password has been changed successfully" ,change the password in the users table, and send an email to the administrator email with the new password	Valid
7	Change administrator email	*Same as change password testing*		Valid
8	Password recovery	Press password recovery in the administrator "account settings" page	Send an email to the administrator email with the current password	Valid
9	Archive Remote PCs' details	Press "Send to archive" button in the PC details page	Send a copy of the viewed PC's details to PC details table in RNMS database	Valid
10	Logout	Press "logout" button at any	Change the	valid

		page	administrator status to "logged out" and redirect the administrator to the "login" page	

5.2.3 RNMS System Testing

A system testing comes after the integration testing. In this stage all the system modules will be integrated together and the whole system will be tested to check the system serviceability in general and in particular, ensuring the testing of maximum system workload, a configuration and its dynamic changes, a performance and a capacity, a system readiness, facilities of error detection and correction, and the security. (Samvel et al., 1995)

For the purpose of the RNMS system test, the whole system was tested in computer lab (BIT2) in UUM University. The test lasted about three hours under the supervision of all most all the labs supervisors in the department of Information Technology. 10 PCs were involved in the

testing. A laptop with 1.73 Due Core CPU, and 2 Gaga Byte RAM was used as a web server (IIS server) and a database server (SQL). The testing summary is shown in table5.2

Table5.2: RNMS System Testing Summarized

Testing type	Evaluation
Configuration	The system was perfectly running without changing any configuration
Performance and Respond time	The system responded was slow due to the limitation of the server hardware specifications (My own laptop)
Security	The system security was acceptable
Reliability	Acceptable
Functionality	The system respond perfectly in performing all the main functional requirements

5.3 RNMS Validation Test

Validation testing aims to check that the software is satisfies the intended usage. On other words, to check "whether you build the right system". In order to preserve the validation of software a user satisfaction test is

conducted. Alireza et al. (2009) argues that among several models of testing user satisfaction Technology Acceptance Model (TAM) is the most widely used one. Based on TAM model there are two main factors influence the user satisfaction; Preserved Usefulness (PU), and Preserved Ease of Use (PEU). (William M., 2004)

Salvador and Jose (2006) illustrated that Preserved Usefulness (PU) test the degree of which a person believes that using a system will enhance his/her job performance. While PEU test the degree of which a person believes that using a particular system will be very ease (free of offer). To evaluate the user acceptance of the proposed RNMS a field study used to carry out this process. Details are below.

5.3.1 Instrument

Based on TAM model, a survey instrument consisted of 10 items was developed to evaluate PU and PEU of the proposed system (The first four items evaluate the Usefulness while the second four items test Ease of use). A six-point liker scale was used to measure respondents' agreement or disagreement from 1 (Strongly disagree) to 6 (strongly agree). The adopted questioner is attached at Appendix E page 156.

5.3.2 Participants and data collection

A total of 15 questioners were distributed, and all were collected. All respondents were IT related people. 80% of the respondents were experts in network management (computer lab supervisors and network lecturers in UUM University). Data collection leaded 5 days from 15th Oct to 19th Oct 2009.

5.3.3 Data Analysis

SPSS (Statistical Package for the Social Sciences) Version16.0 has been used to analysis the participants respondents. Figure5.1 shows the respondents' academic backgrounds.

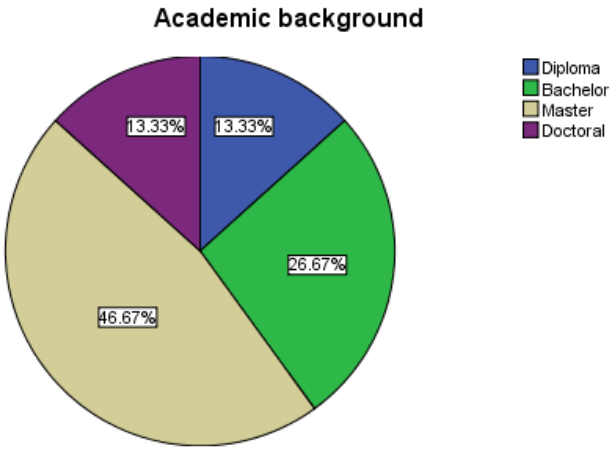


Figure5.1: Respondents academic background

5.3.4 Results

Descriptive statistics are used to describe the collected data analysis results. As illustrated in section 5.3.2 the questioner tries to evaluate the PU and PEU. The following two sections describe the Descriptive statistics of both PU and PEU.

5.3.4.1 PU (Preserve Usefulness) Descriptive Statistics

The responses of the first four items of the questioner test the Usefulness of RNMS. Table5.3 shows the number of respondents (N), minimum and maximum respond, and mean of the RNMS Usefulness.

Table5.3: RNMS Usefulness Descriptive Statistics

	N	Minimum	Maximum	Mean
Q1	15	3	6	4.33
Q2	15	3	6	4.53
Q3	15	3	6	4.20
Q4	15	3	6	4.33

According to the results shown in the previous table, the Mean values (the average) of the four questions are above 4 (Agree).

That is mean; the system usefulness is agreed by all the respondents.

5.3.4.2 PEU (Preserve Ease of Use) Descriptive Statistics

Preserve Ease of Use measured by the responses of the second four items of the questioner. The results are shown is table5.4.

Table5.4: RNMS PEU Descriptive Statistics

	N	Minimum	Maximum	Mean
Q5	15	4	6	4.47
Q6	15	4	6	4.60
Q7	15	4	6	4.47
Q8	15	4	6	4.60

As shown in table5.4; the average of the responses is above 4 (Agree) which indicate that the ease of use RNMS system is agreed.

The complete descriptive statistics of the questioner's data analysis is attached at Appendix F page 158.

5.3.5 Discussion

The results of the data analysis process indicated that; the users agreed about the usefulness and the ease of use of the proposed system. As a result, the users accept the proposed system. However, the respondents puttied forth some comments and suggestions as listed below;

- Improve the produced repots and charts
- Provide some control functions (like; Shutdown or restart nodes)
- Improve the system ability to automate the generating of the PC list

5.4 Summary

This chapter described the process of evaluation the RNMS. Two phases of testing were performed to evaluate the proposed system, Validation test and Verification test. During the verification phase the system was tested in three stages; the unit testing, the integration testing, and the system testing. Black box testing has been used to test the integrity of the RNMS modules. The second phase of testing has been started after the system was passed the verification test. In the second phase the validation test has evaluated the users' acceptance of the proposed system. A user survey based on TAM model

has been adopted to test the RNMS usefulness and ease of use. SPSS used to analysis the collected data. The results after the analysis indicated that the users accepted the proposed system.

CHAPTER SIX

CONCLUSION

6.1 Introduction

This chapter will conclude the research results, present the study limitations, discuses the recommendations and the future work.

6.2 Achievements

Referring back to the objectives of this study;

- To design a web-based management system to monitor all the computers within a network.
- To develop a prototype of the proposed system
- To test and evaluate the prototype and its usability

The logical and the physical design of the RNMS were discussed abundantly in chapter tow, three, and chapter four. Then, the prototyping process was conducted in chapter four. Chapter five then fulfilled the testing and the

evaluation process. Thus, It can be concludes that the project's objectives have been accomplished successfully.

6.3 RNMS Strengths

RNMS offers numerous towards of the computer networks managers. Listed below are some benefits of using RNMS;

- The developed RNMS model is a general model because the model is based on a UML. Here, object oriented concept (reusable model) will offer a good starting point when new SNMP based application is encountered.
- RNMS provides a simple way to get the current status of the network's PCs.
- RNMS is a web application meaning that; you can access the RNMS anytime anywhere.
- RNMS is based on SNMP (Simple Network Management Protocol). SNMP is now in widespread use. Most major operating systems and vendors of network hardware -workstation, bridges, routers, and etc. - offer the basic SNMP compatibility.
- SNMP provides a high level of secure transmission.

6.4 RNMS Limitations

However, the study objectives have been accomplished successfully within the given short time. This agile development of such application will led to some limitations. Some of these limitations are listed below;

- The developed system lacks of some additional monitoring functions. For example; alarms monitoring and managing.
- The scope of the study focused on monitoring networks' hosts. However, other devices (such as; hubs, routers, printers, and etc.) have to monitor in order to develop a complete network monitoring system.
- The system lacks of providing professional reports.
- The limitations of using SNMP (some limitations of retrieving large volumes of data)
- The complexity of network environments.

6.5 Future work

Some future enhancements and recommendations listed below;

- Expand the study scope to cover monitoring all the network's components. The hardware components such as; hubs, routers, printers, and etc. As well as the software components such as; database services and etc.

- Expand the functionality of the system by adding some control functions. Such as; remotely shutdown and restart a device, a software, or even a process.
- Include monitoring and mange the network faults. Or even predict the fault before it happened.

6.6 Summary

This chapter discussed the study achievements, strengths, limitations, and future works. It has concluded that the study objectives have been accomplished successfully. However, some limitations and constraints confined the findings of the study. Basically, the scope, short time, and the complexity of the study are the most challenges faced the researcher during this project.

Hopefully, the RNMS will be a good starting point for new network management applications.

References:

Prabhu S, & Venkat R. (2007). High Availability for Network Management Applications. *IEEE*

Raouf B., & Andreas P., (2001). Projection FCAPS to Active Network. *IEEE*.

Douglas M., & Schmidt, K. (2001). *Essential SNMP*. O'Reilly.

Fábio Luiz Leite Jr, André Gomes de Sousa, Cláudio de Souza Baptista, Camilo Porto Nunes, Elvis Rodrigues da Silva, Damião Ribeiro de Almeida, et al. (2005). Migratool: Towards a Web-Based Spatial Database Migration Tool. *IEEE*.

Rong-Ceng Leou, & Zwe-Lee Gaing. (2002). A Web-Based Load Flow Simulation of Power Systems. *IEEE*.

Alexander clemm. (2007). *Network Management Fundamentals*. Indianapolis: Cisco Press.

Zhang Yongjun, & Jiang Dingfu. (2008). Web-Based Network Management System Revolving About Database. *IEEE*.

Hwa-chun lin, & chien-hsing wang. (1999). Distributed network management by http-based remote invocation. *IEEE*.

FLEXTORONICS. (2005). FACPS [Electronic Version] from http://stockrt.homelinux.com:8080/ger/fcapswp.pdf.

Prabhu S, & Venkat R. (2007). High Availability for Network Management Applications. *IEEE*.

Mouhammd Al-Kasassbeh, & Mo Adda. (2009). Network fault detection with Wiener filter-based agent. *Journal of Network and Computer Applications*.

Laxman Sahasrabuddhe, S. Ramamurthy, & Biswanath Mukherjee. (2002). Fault Management in IP-Over-WDM Networks: WDM Protection Versus IP Restoration. *IEEE*.

Kinga, & R. Huntb. (2000). Protocols and architecture for managing TCP/IP network infrastructures. *Computer Communications*.

Gary Audin, & Fiona Lodge. (2006). FCAPS: A Model For VOIP/IPT Management. *BUSINESS COMMUNICATIONS REVIEW*.

William Stallings. (1993). *SNMP, SNMP2, and CMIP the practical Guids to Network Management Standards* (5th ed.): Addison-Wesley Publishing Company.

Raouf Boutaba, & Andreas Polyrakis. (2001). Projecting FCAPS to Active Networks. *IEEE*.

Yuan Zhang, Gaochao Xu, & Xiaozhong Geng. (2008). Security Threats in Active Networks. *IEEE*.

Douglas M., & Schmidt, K. (2001). *Essential SNMP*: O'Reilly

J. Case, M. Fedor, M. Schoffstall, & J. Davin. (1990). A Simple Network Management Protocol (SNMP) [Electronic Version]. *RFC1157*.

CISCO Systems. Simple Network Management Protocol (SNMP) [Electronic Version]. *Internetworking Technology Handbook* Retrieved September 23, 2009 from http://www.cisco.com/en/US/docs/internetworking/technology/handbook/SNMP.pdf.

Wenxian Zeng, & Yue Wang. (2009). Design and Implementation of Server Monitoring System Based on SNMP. *IEEE*.

M. Sarram, M. ghasemzadeh, & V. Aghaei. (2008). Remote Control and Overall Administration of Computer Networks, Using Short Message Service. *IEEE*.

Amatzia Bent-Artzi, Asheem Chandna, & Unni Warrier. (1991). Network Management of TCP/IP Networks: Present and Future. *IEEE*.

Zhen-qi WANG, Yue WANG, & Guangqiang SHAO. (2009). Research and Design of Network Servers Monitoring System Based on SNMP. *IEEE*.

F.G. Hatefi, & F. Golshani. (1999). A new framework for secure network management. *Computer Communications*.

Matthias Wiesmann, P´eter Urb´an, & Xavier D´efago. (2006). An SNMP based failure detection service. *IEEE*.

K. McCloghrie. (1991).Management Information Base for Network Management of TCP/IP-based internets:MIB-II. *RFC1213*

Vaishnavi, V. and Kuechler, W. (2004).“Design Research in Information Systems,” January 20, 2004; last revision on February 20, Retrieved July 10, *2009*, from http://www.isworld.org/Researchdesign/drisISworld.htm

Naumann, Justus D., and A. Milton Jenkins. "Prototyping: The New Paradigm for Systems Development." MIS Quarterly , 6, No. 3 (1982),29-44.

V. Scott Gordon, & James M. Bieman. (1995). Rapid Prototyping: Lessons Learned. *IEEE*.

Knight,L., Steinbach,T.,Kellen,V.,(2001). System Development Methodologies for Web Enabled E-Business: A Customization Paradigm. Retrieved January 16, 2005, from http://www.kellen.net/SysDev.htm

Sommerville, I. (2007). *Software engineering*. International computer science series. Boston: Pearson/Addison-Wesley.

Bahrami, A. (2000). Object Oriented System Development Using Unified Modeling Language. Boston: McGraw-Hill Book Company.

Donald C. Gause, & Gerald Weinberg. (1989). *Classic Book Review: Exploring Requirements: Quality Before Design*: Dorset House.

Simon Bennett, Steve McRobb, & Ray Farmer. (2006). *Object-Oriented System Analysis and Design* (3rd ed.). Berkshire: MCGraw-Hill Education.

Dennis, A., Wixom, H., & Tegarden, D. (2005). *System analysis and design with UML version 2.0: an object-oriented approach with UML, 2nd edition*. Hoboken, NJ: John Wiley and Sons, Inc.

Dmitry E. Tananko, Sharad Kumar, & John Paulson. (2009). Reliability Growth of Mobile Gun System during Production Verification Test. *IEEE*.

Preston Pierce. (1995). Software Verification & Validation. *IEEE*.

Doron Drusinsky, James Bret Michael, Thomas W. Otani, & Man-Tak Shing. (2005). Validating UML Statechart-Based Assertions Libraries for Improved Reliability and Assurance. *IEEE*.

Beydeda, S. (2005). Self-testability in Unit Testing. *IEEE*.

Bin Xu. (2009). Towards Efficient Collaborative Component-based Software Unit Testing via Extend E-CARGO Model-based A ctivity Dependence Identification. *IEEE*.

Board, I. S. (1986). IEEE Standard for Software Unit Testing. *IEEE*.

Ursula Linnenkugel, & Monika Mullerburg. (1990). Test Data Selection Criteria for (Software) Integration Testing. *IEEE*.

Ma Liangli, Wang Houxiang, & Li Yongjie. (2007). A Reference Model of Grouped-Metadata Object and a Change Model based on it Appling for Component-based Software Integration Testing. *IEEE*.

Tafline Murnane, & Karl Reed. (2001). On the Effectiveness of Mutation Analysis as a Black Box Testing Technique. *IEEE*.

Harrine Freeman. (2002). software testing. *IEEE*.

Samvel K. Shoukourian, Armen G. Kostanian, Valery A. Margarian, & Ayman A. Ashour. (1995). An Approach for System Tests Design and Its Application. *IEEE*.

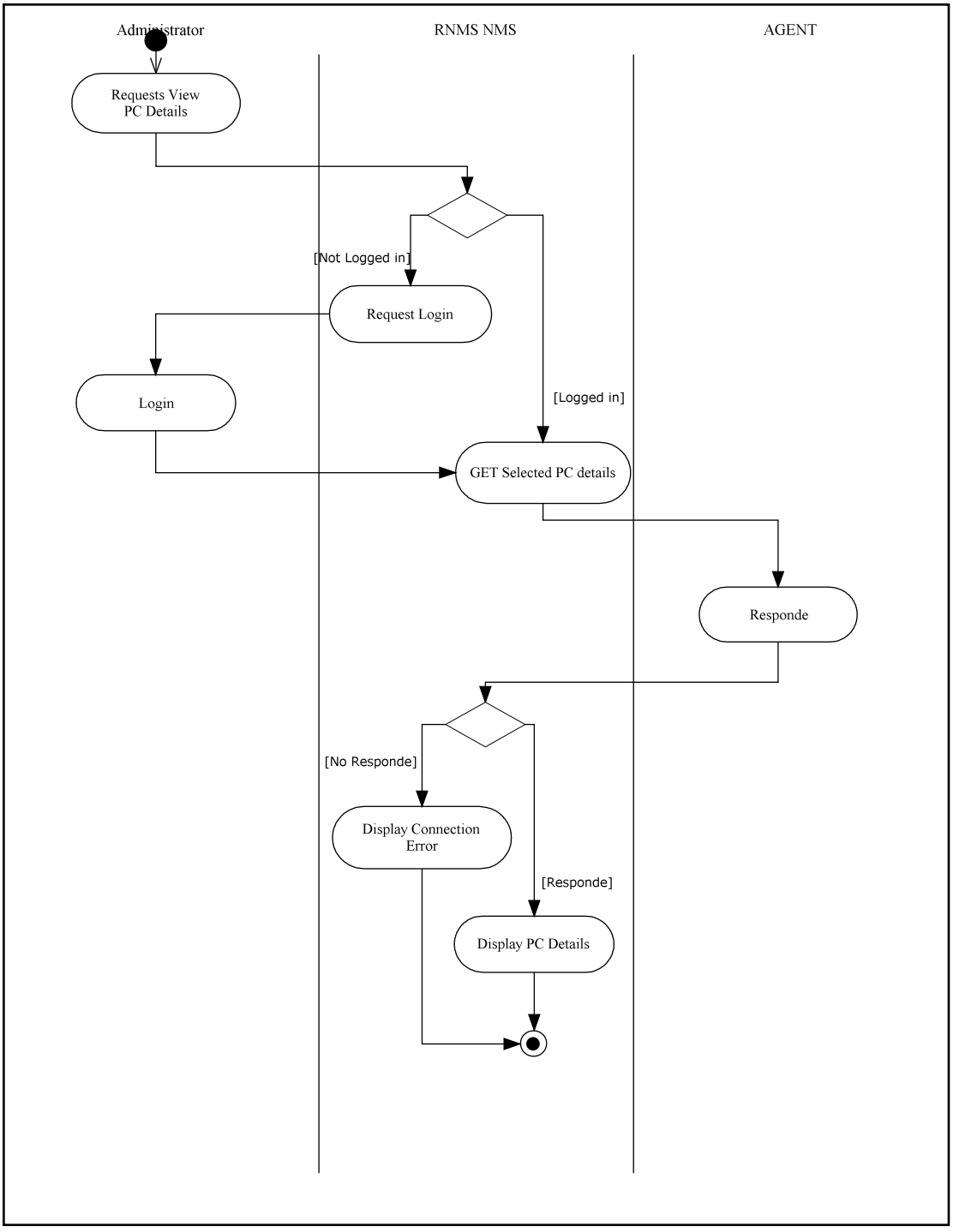
William Money. (2004). Application og the Technology Acceptance Model to Knowledge Management System. *IEEE*.

Alireza Talebpour, Sona Bairamzadeh, & Seyed Sabah Vajdi. (2009). Extending the Technology Acceptance Model for Internet Banking:A Case Study of Iran. *IEEE*.

Salvador Bueno, & Jose L. Salmeron. (2006). TAM-based success modeling in ERP. *Interacting with Computers*.

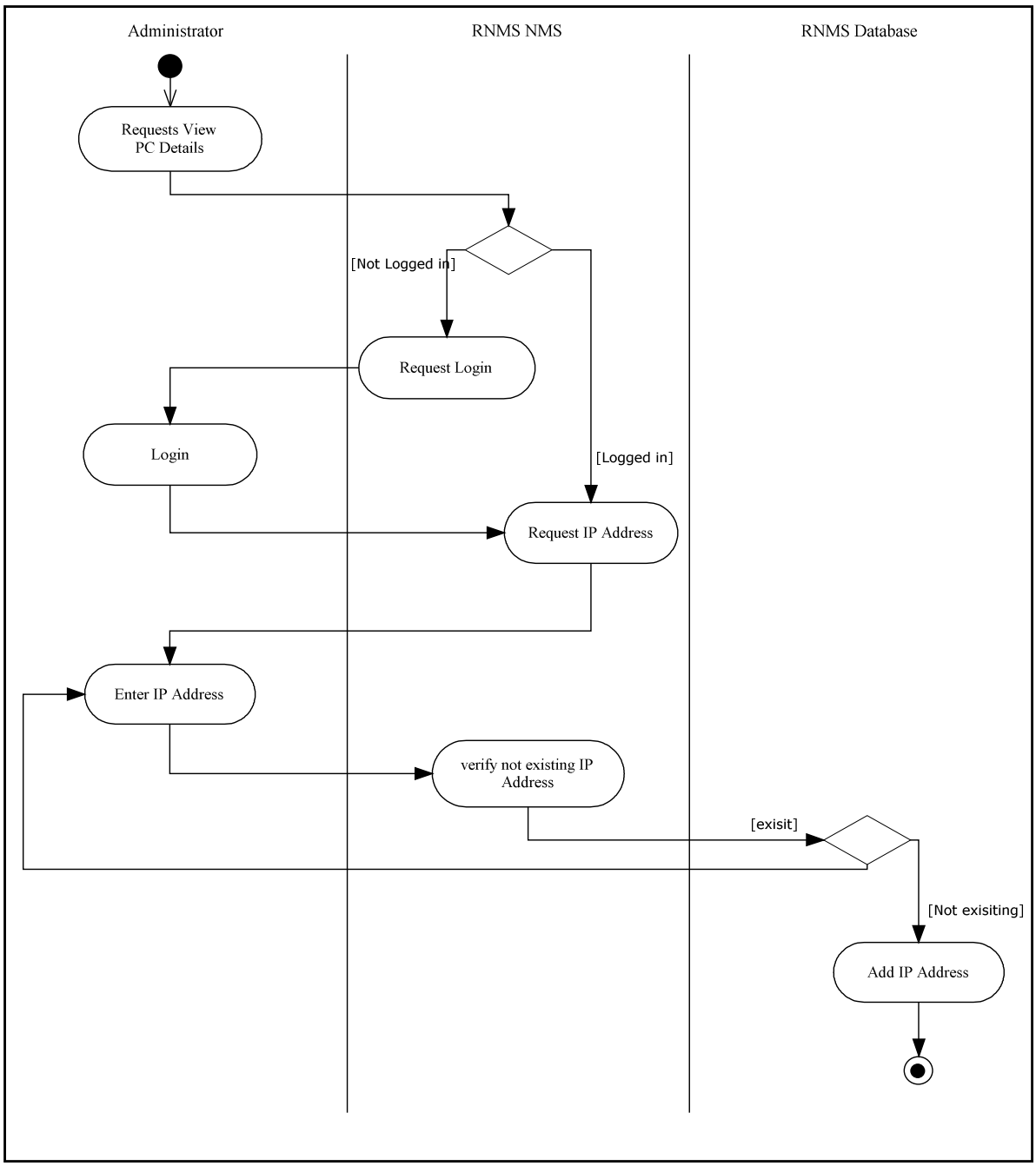
APPENDIX A
RNMS ACTIVITY DIAGRAMS

REMOTE SYSTEM MANAGEMENT SYSTEM (RNMS)
View PC Details

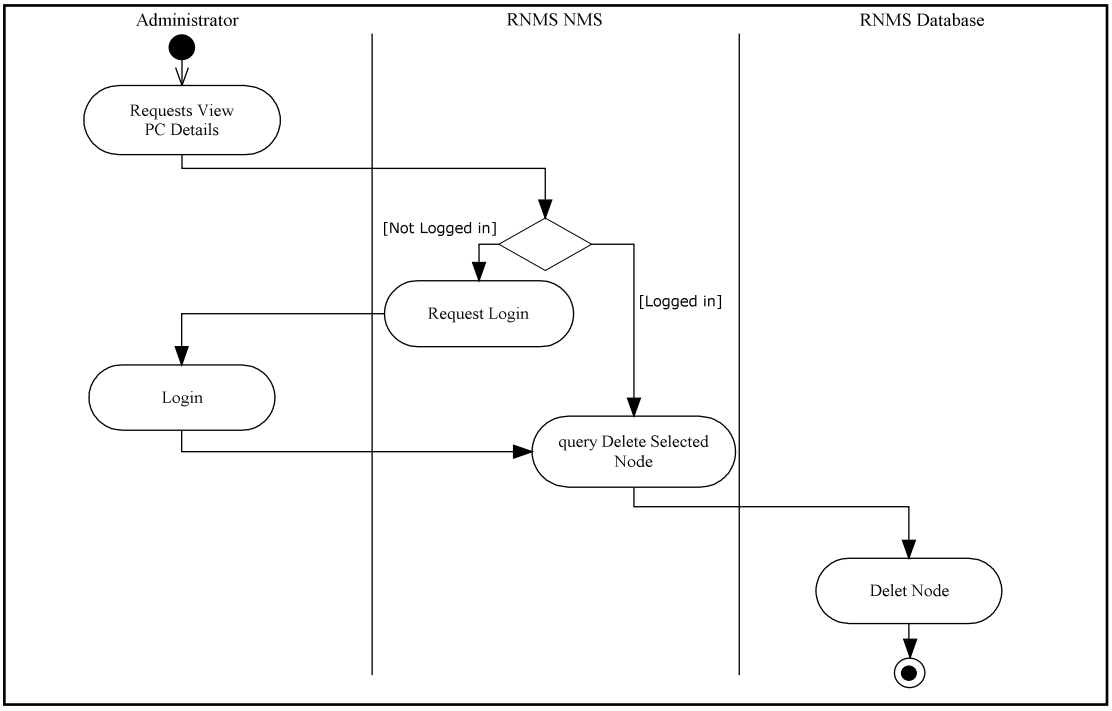


REMOTE SYSTEM MANAGEMENT SYSTEM (RNMS)

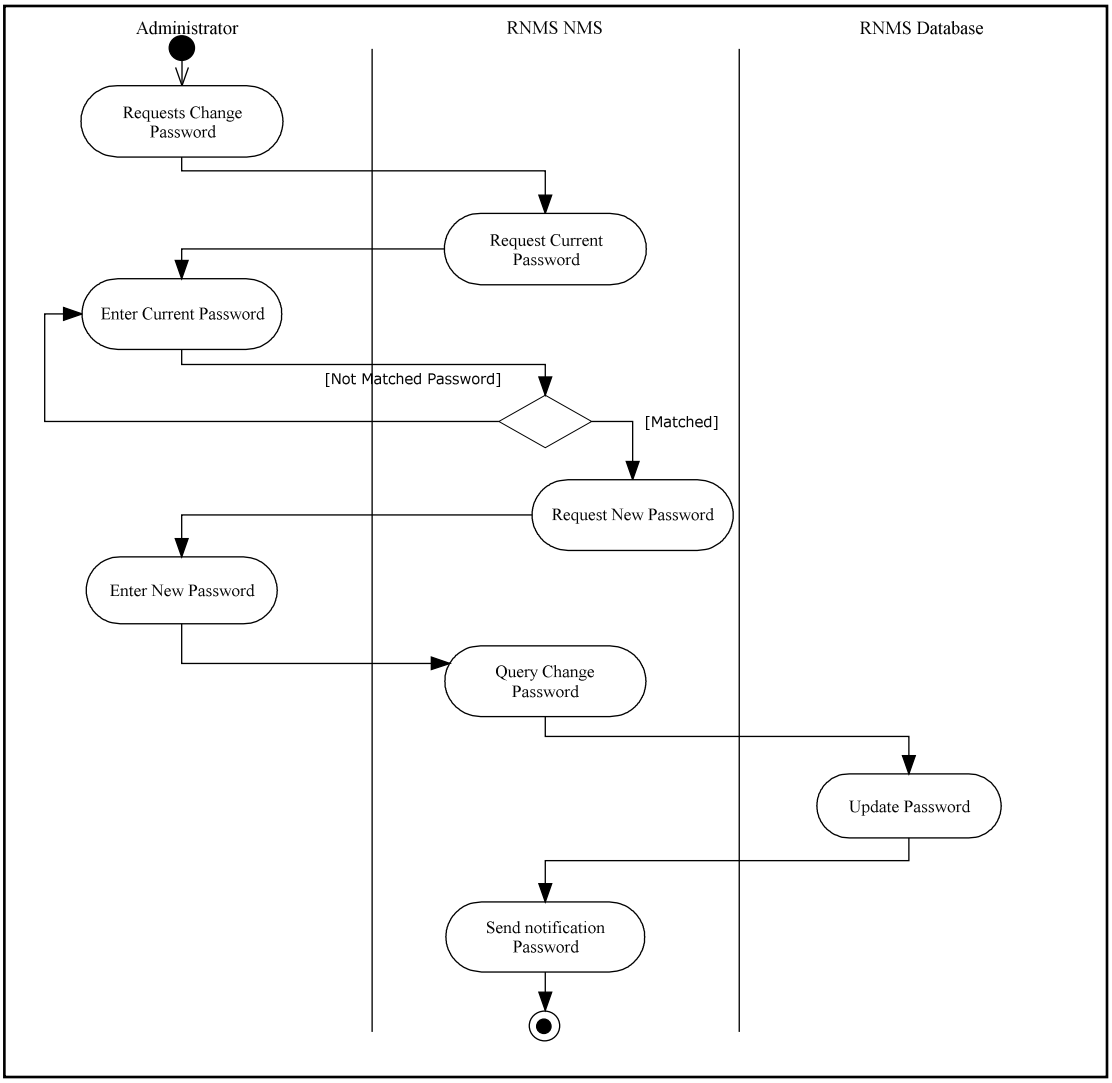
Add New PC



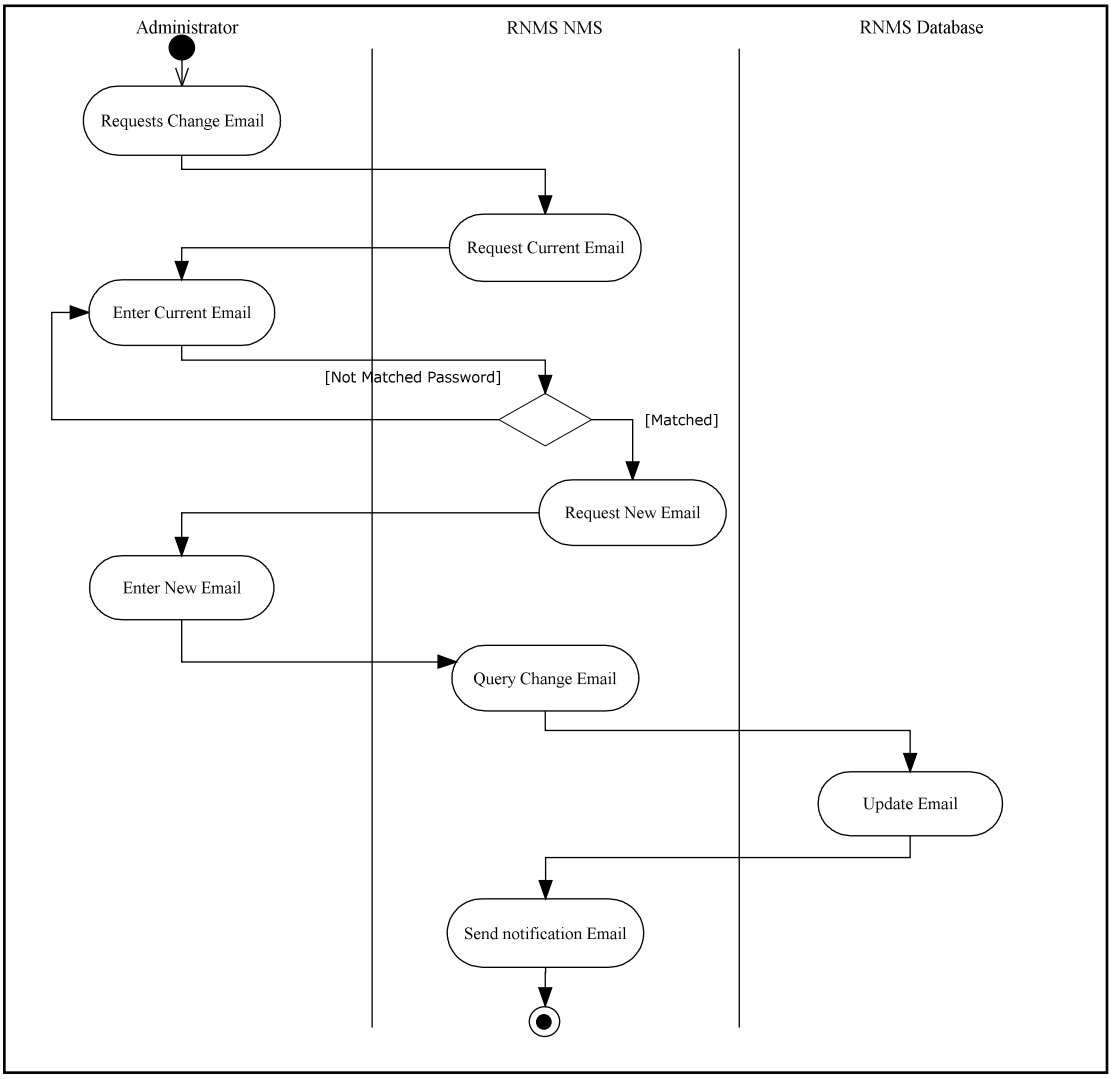
REMOTE SYSTEM MANAGEMENT SYSTEM (RNMS)
Remove PC



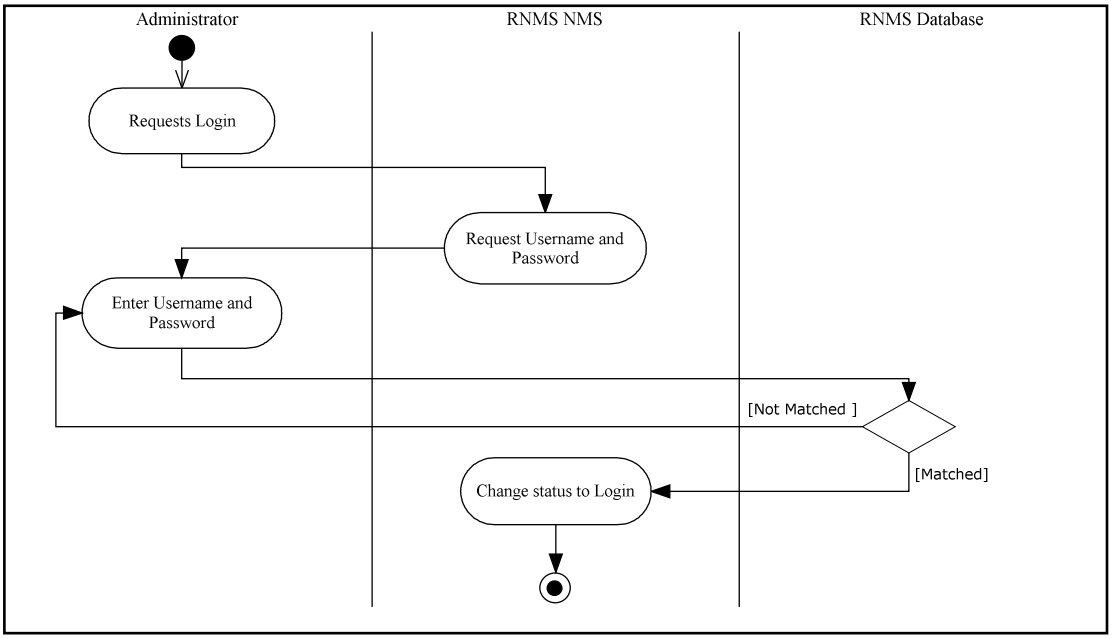
REMOTE SYSTEM MANAGEMENT SYSTEM (RNMS)
Change Administrator Password



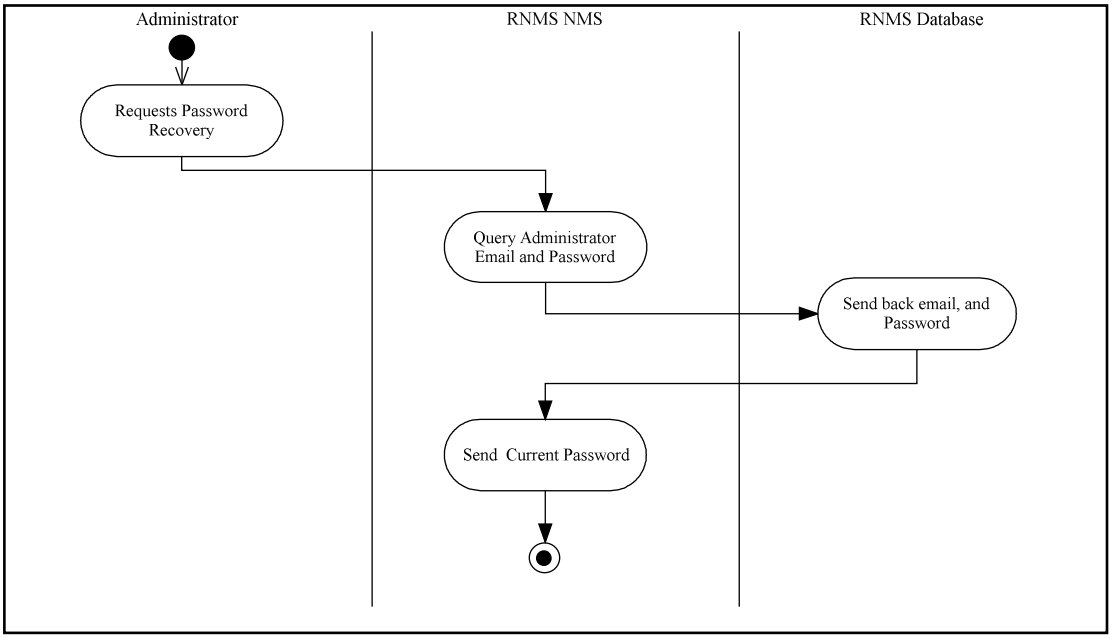
REMOTE SYSTEM MANAGEMENT SYSTEM (RNMS)
Change Administrator Email



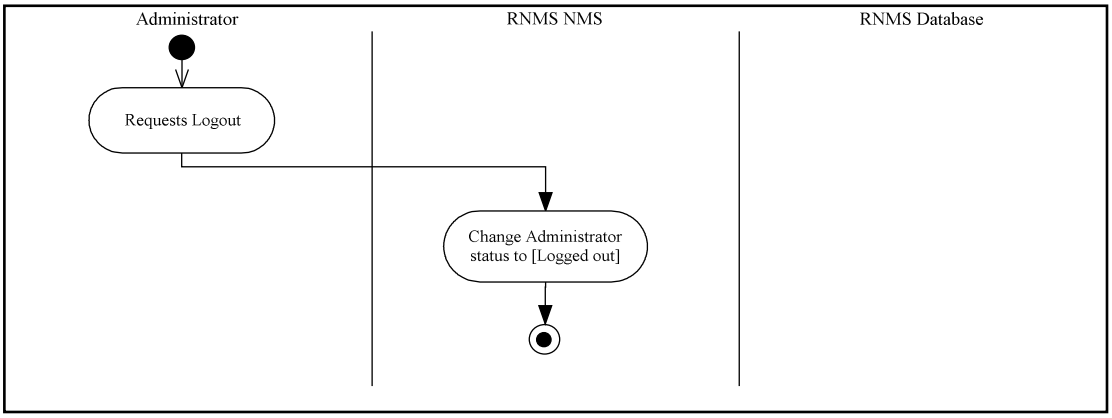
REMOTE SYSTEM MANAGEMENT SYSTEM (RNMS)
Login Activity Diagram



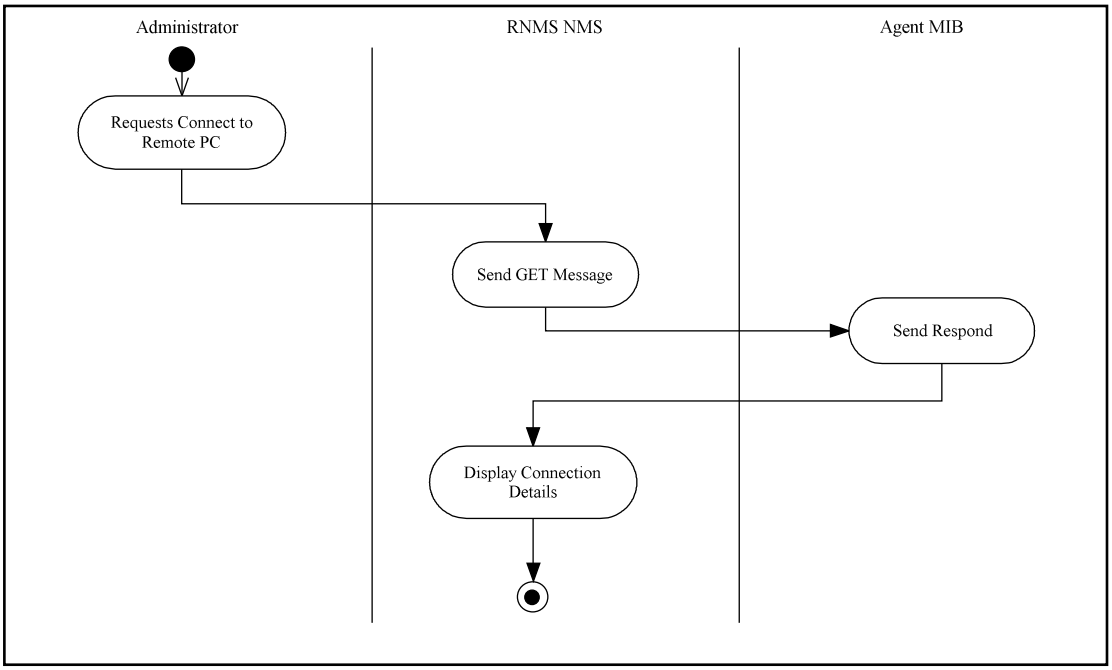
REMOTE SYSTEM MANAGEMENT SYSTEM (RNMS)
Password Recovery Activity Diagram



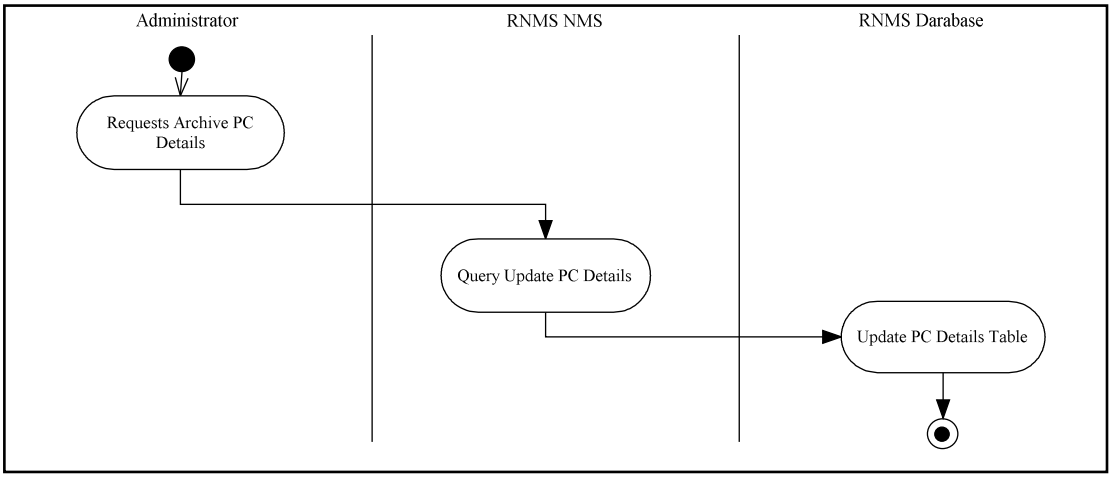
REMOTE SYSTEM MANAGEMENT SYSTEM (RNMS)
Logout Activity Diagram



REMOTE SYSTEM MANAGEMENT SYSTEM (RNMS)
Connect to Remote PC Activity Diagram

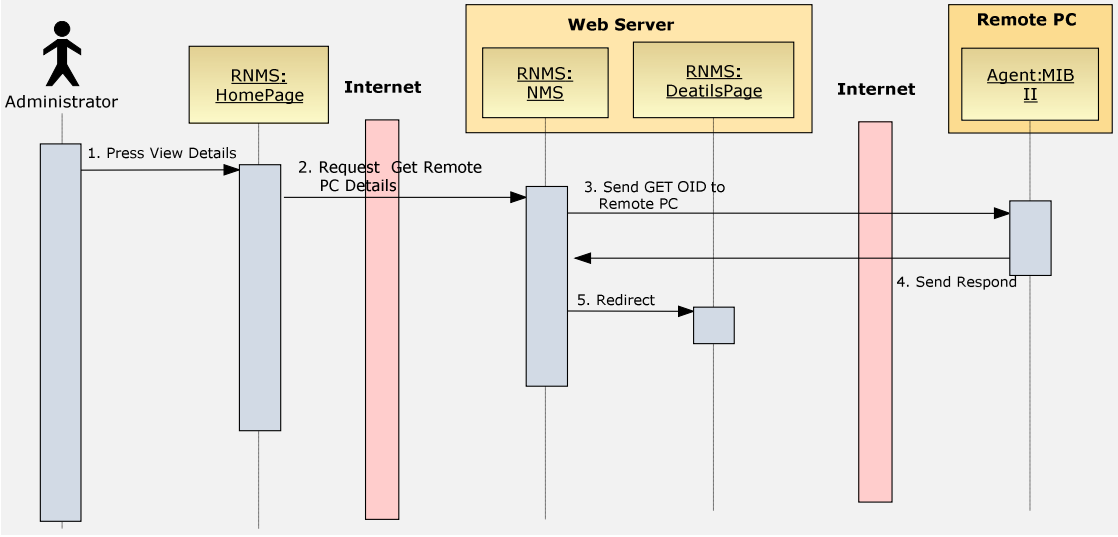


REMOTE SYSTEM MANAGEMENT SYSTEM (RNMS)
Archive PC Details Activity Diagram

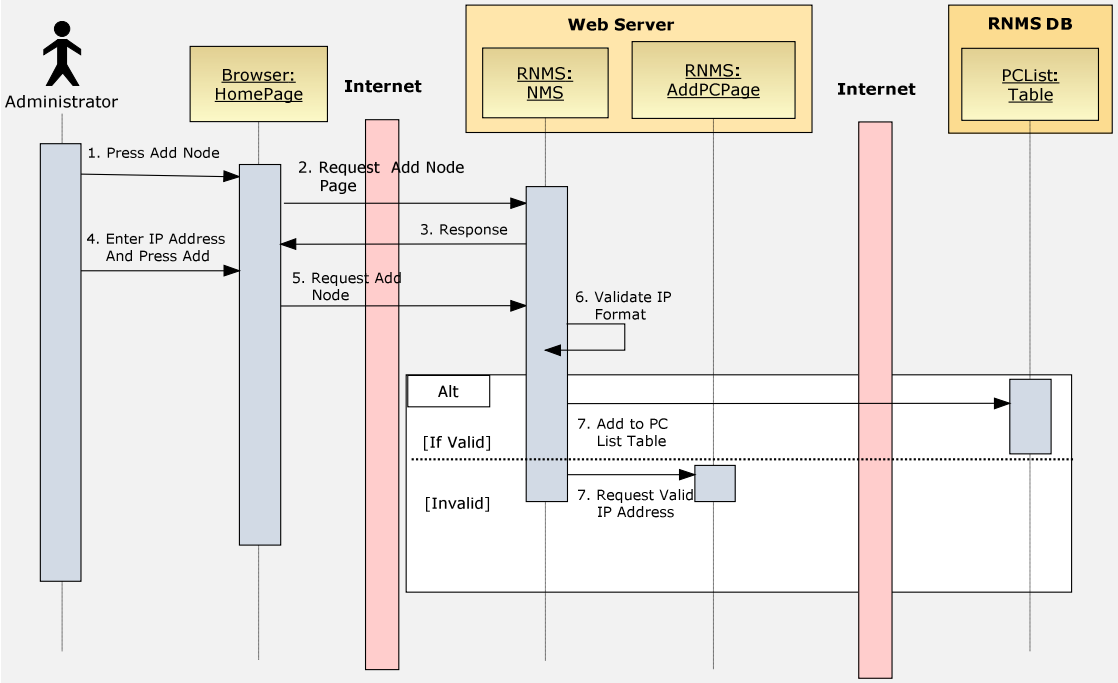


APPENDIX B
RNMS SEQUENCE DIAGRAMS

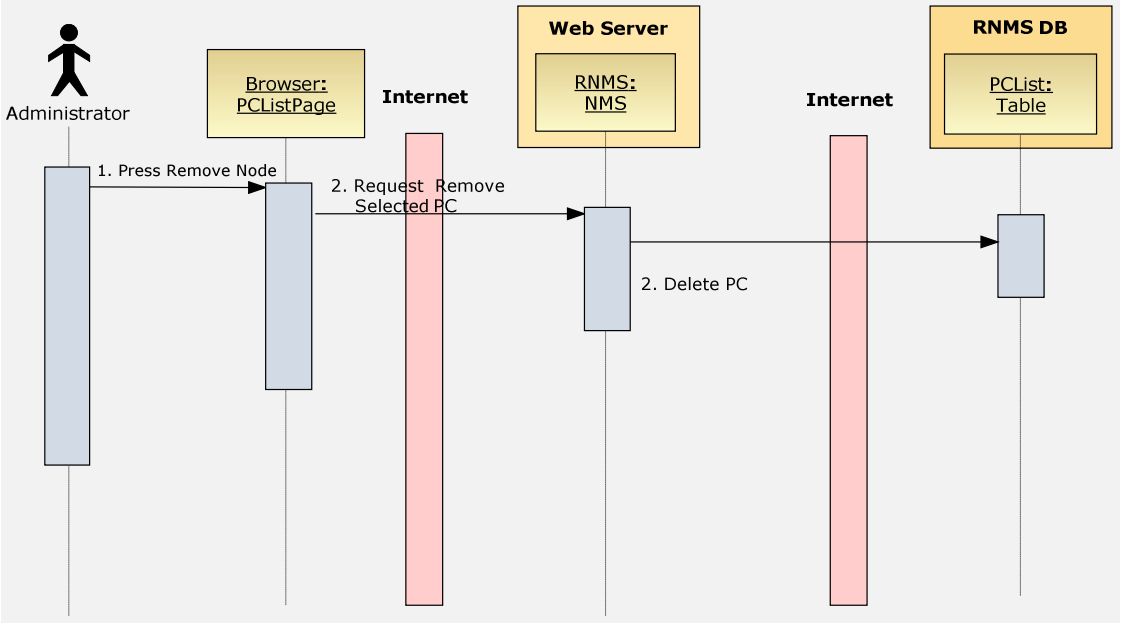
VIEW REMOTE PC DETAILS SEQUENCE DIAGRAMS



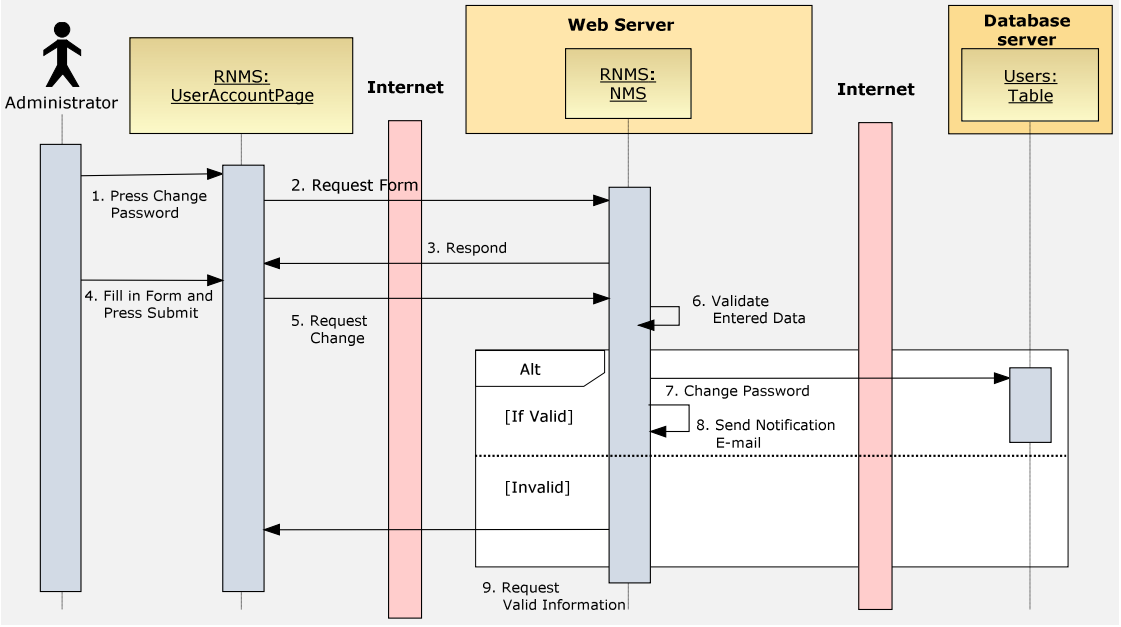
ADD NEW PC SEQUENCE DIAGRAMS



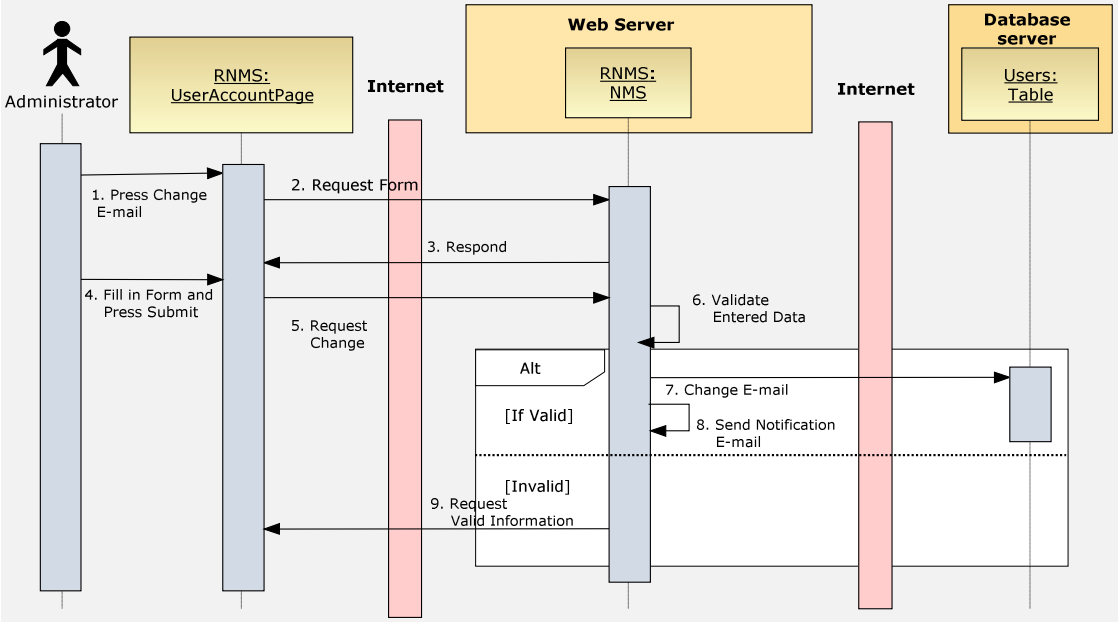
REMOVE PC SEQUENCE DIAGRAMS



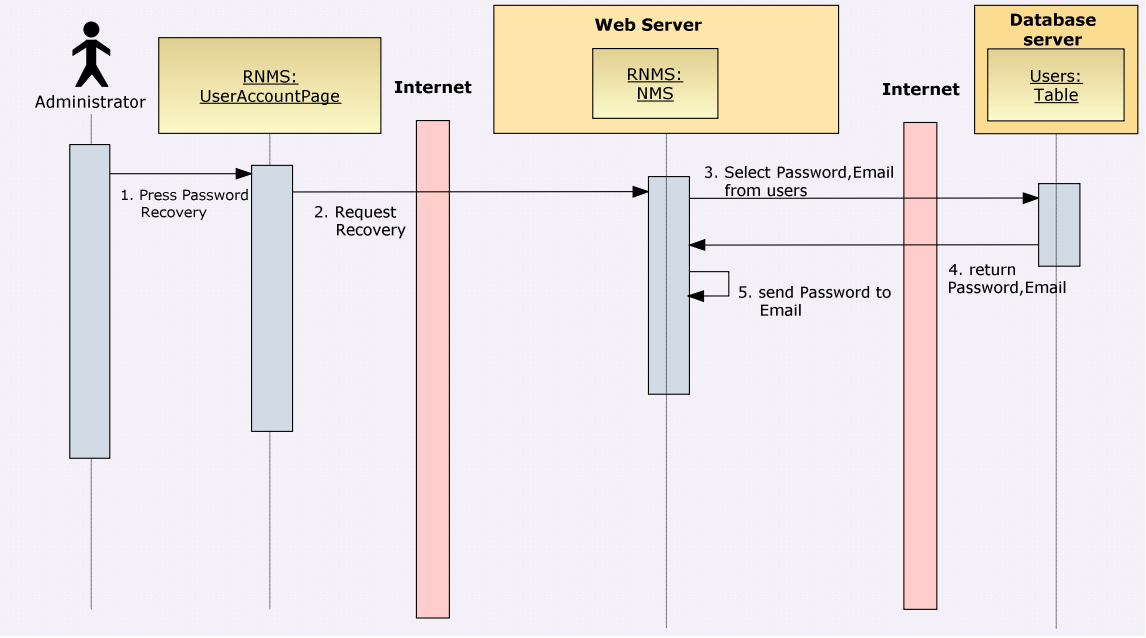
CHANGE PASSWORD SEQUENCE DIAGRAMS



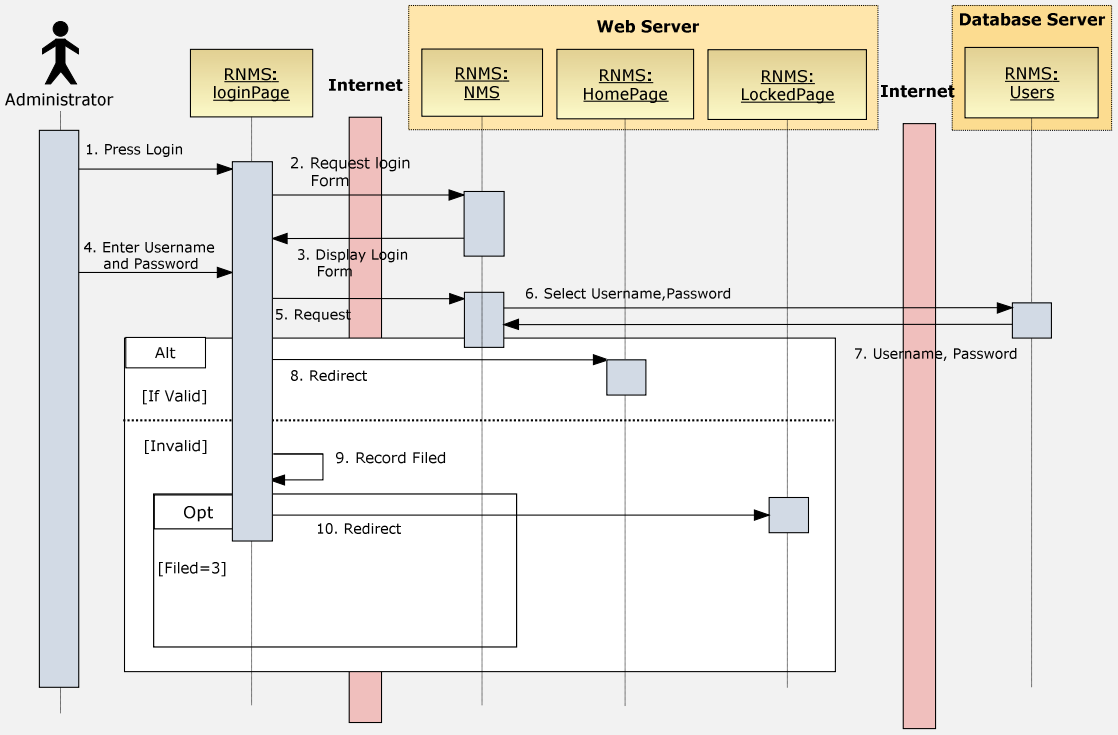
CHANGE E-MAIL SEQUENCE DIAGRAMS



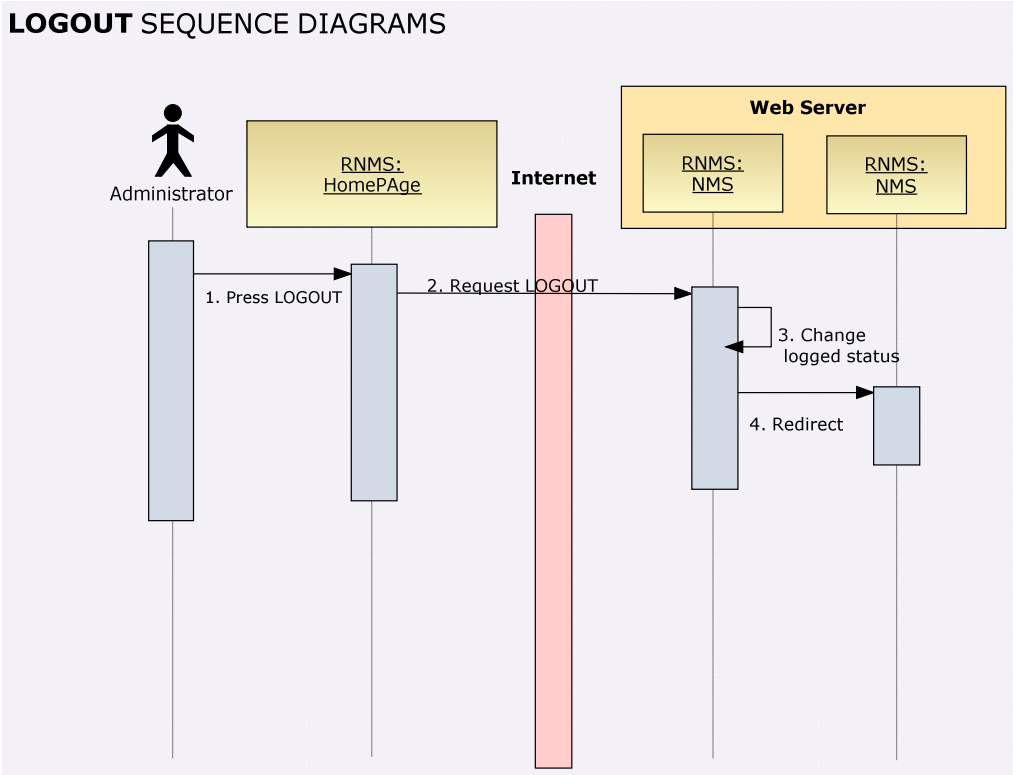
PASSWORD RECOVEY SEQUENCE DIAGRAMS



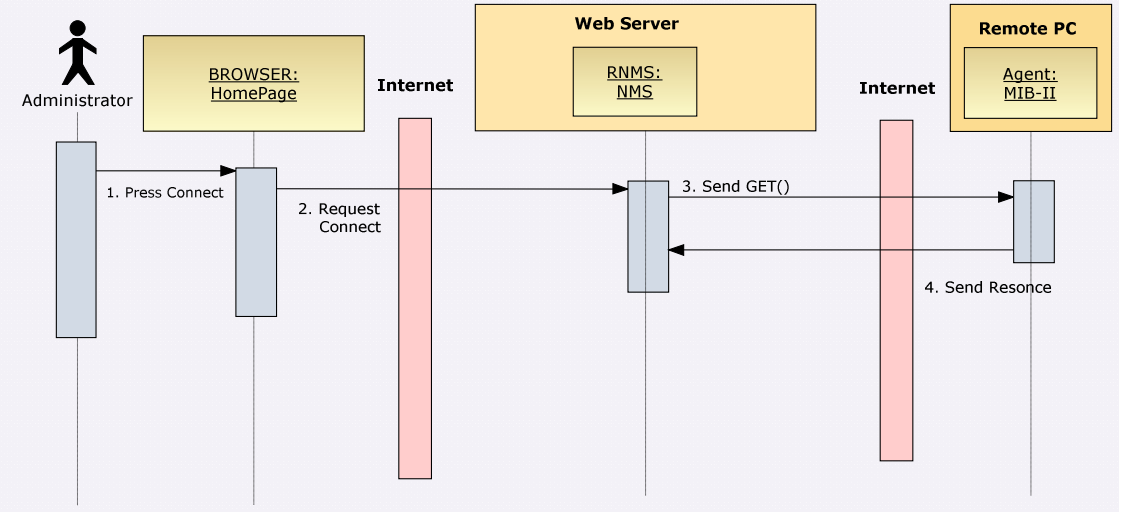
ADMINISTRATOR LOGIN SEQUENCE DIAGRAM



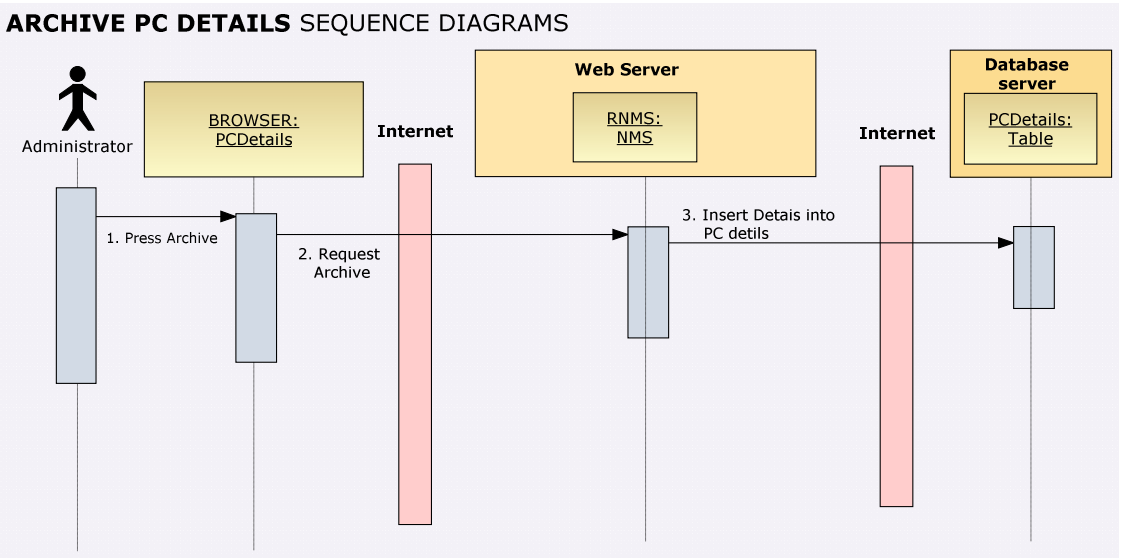
LOGOUT SEQUENCE DIAGRAMS



CONNECT TO REMOTE PC SEQUENCE DIAGRAMS



ARCHIVE PC DETAILS SEQUENCE DIAGRAMS

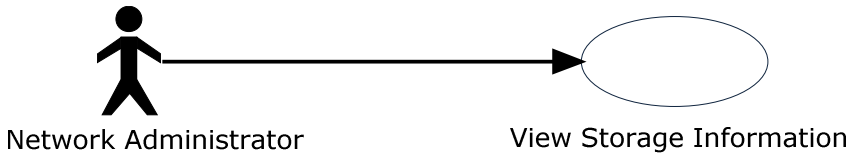


APPENDIX C

RNMS USE CASE SPECIFICATION

Following are the complete use case specifications;

USE CASE: View Storage Information (RNMS_01_02)



BRIEF DESCRIPTION

This use case is initiated by the network administrator. This use cannot be initiated unless the administrator has a successful login to the system. This use case enable network administrator to view Storage information about the monitored PC, Storage description, storage allocation unit (byte), storage total size (GByte), used size (Gbyte), free space (Gbyte), and storage label.

PRE-CONDITIONS

- Administrator must be logged in
- The system has successfully connected to the remote PC

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the administrator presses on the “Storage” navigation button in the home page main menu.

- If the system successfully connects to the remote PC (using the IP chosen by the user) the system shall display Storage Information about the connected PC on the screen.
- The administrator can view updated information about the remote PC storage by press the "Refresh" button to re-connect again with the remote PC and get storage's current status.
- The administrator can press "Save to Archive" button to initiate the **Archive Storage Information USE CASE (RNMS_07_02).**
- If the system could not connect to the remote PC successfully then the system shall display a message to inform the administrator about what error was happened. (Exception follow **E1)**

Alternative Flow

Not Applicable.

Exceptional Flow

E-1: Connection Error (RNMS_01_01_01)

The system shall display a message about what error was happened while trying to connect to the remote PC. The system shall not show the "**Save to Archive**" button.

E-2: Web Server Error (RNMS_01_01_02)

If the server is crash then the system shall display "**The Server is Down**" button.

POST-CONDITIONS

The administrator be able to archive what information the system is display about the remote PC.

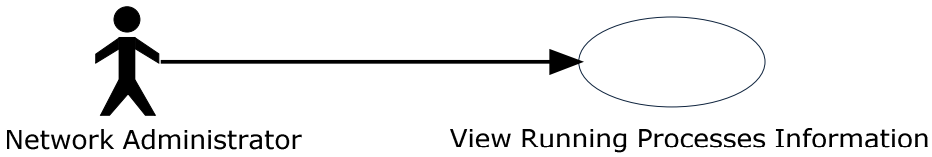
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable.

USE CASE: View Running Processes Information (RNMS_01_03)



BRIEF DESCRIPTION

This use case is initiated by the network administrator. This use cannot be initiated unless the administrator has a successful login to the system. This use case enable network's administrator to view monitored PC's Running Processes information; Process name, process's application path (of course the path on the monitored PC), process status (idle , active, and etc.), the process CPU usage, and process memory usage(RAM).

PRE-CONDITIONS

- Administrator must be logged in
- The system has successfully connected to the remote PC

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the administrator presses on the "Running Processes" navigation button in the home page main menu.

- If the system successfully connects to the remote PC (using the IP chosen by the user) the system shall display running services Information about the connected PC on the screen.
- The administrator can view updated information about the remote PC running processes by press the "Refresh" button to re-connect again with the remote PC and get storage's current status.
- The administrator can press "Save to Archive" button to initiate the **Archive Processes Information USE CASE (RNMS_07_03).**
- If the system could not connect to the remote PC successfully then the system shall display a error message to inform the administrator about what error was happened. (Exception follow **E1)**

Alternative Flow

Not Applicable.

Exceptional Flow

E-1: Connection Error (RNMS_01_01_01)

The system shall display a message about what error was happened while trying to connect to the remote PC. The system shall not show the "**Save to Archive**" button.

E-2: Web Server Error (RNMS_01_01_02)

If the server is crash then the system shall display "**The Server is Down**" button.

POST-CONDITIONS

The administrator must be able to save running processes information to the running processes information's archives (RNMS_02_03).

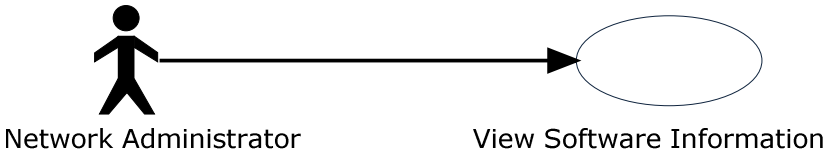
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable.

USE CASE: View Installed Software Information (RNMS_01_04)



BRIEF DESCRIPTION

This use case is initiated by the network administrator. This use cannot be initiated unless the administrator has a successful login to the system. This use case enable network administrator to view a list of the monitored PC's software; software name, and installed date. Also, administrator can arrange the list by the name of the software or by installation date.

PRE-CONDITIONS

- Administrator must be logged in successfully
- System successfully connected to the remote PC

CHARACTERISTIC OF ACTIVATION

Event driven (network administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the administrator presses on the "Software" navigation button in the home page main menu

- If the system successfully connects to the remote PC (using the IP chosen by the administrator) the system shall display software Information about the connected PC on the screen.
- The administrator can view updated information about the remote PC running processes by press the "Refresh" button to re-connect again with the remote PC and get software's current status.
- The administrator can press "Save to Archive" button to initiate the **Archive Software USE CASE (RNMS_07_04).**
- If the system could not connect to the remote PC successfully then the system shall display a error message to inform the administrator about what error was happened. (Exception follow **E1)**

Alternative Flow

Not Applicable

Exceptional Flow

E-1: Connection Error (RNMS_01_01_01)

The system shall display a message about what error was happened while trying to connect to the remote PC. The system shall not show the "**Save to Archive**" button.

E-2: Web Server Error (RNMS_01_01_02)

If the server is crash then the system shall display "**The Server is Down**" button.

POST-CONDITIONS

- Administrator can a list view remote PC's installed software information
- Administrator can rearrange the displayed list by either the software name or installed date

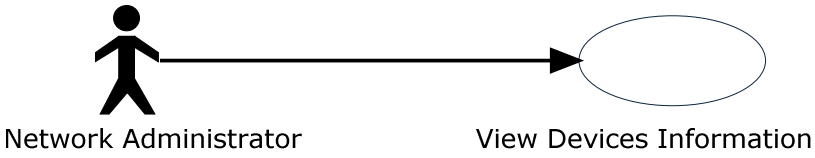
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable.

USE CASE: View Devices Information (RNMS_01_05)



BRIEF DESCRIPTION

This use case is initiated by the network administrator. This use cannot be initiated unless the administrator has a successful login to the system. This use case enable network's administrator to view monitored PC's Running Devices information: Device name, and device current status. Also, network administrator can arrange displayed list by either device name or device current status.

PRE-CONDITIONS

- Administrator must be successfully logged in
- System successfully connected to the remote PC.

CHARACTERISTIC OF ACTIVATION

Event driven (Administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the administrator presses on the “Devices” navigation button in the home page main menu
- If the system successfully connects to the remote PC (using the IP chosen by the administrator) the system shall display remote PC’s devices Information
- The administrator can view updated information about the remote PC’s devices by press the “Refresh” button to re-connect again with the remote PC and get devices current status.
- The administrator can rearranged the displayed list by the device name by clicking the “device name” list header
- The administrator can rearranged the displayed list by the device status by clicking the “device status” list header
- The administrator can press “Save to Archive” button to initiate the **Archive Devices USE CASE (RNMS_07_04)** to send the displayed list to the archive on the RNMS database.
- If the system could not connect to the remote PC successfully then the system shall display a error message to inform the administrator about what error was happened. (Exception follow **E1)**.
- If the administrator is not logged in successfully then the system should redirect the administrator to the login page

Alternative Flow

Not applicable

Exceptional Flow

E-1: Connection Error (RNMS_01_01_01)

The system shall display a message about what error was happened while trying to connect to the remote PC. The system shall not show the "**Save to Archive**" button.

E-2: Web Server Error (RNMS_01_01_02)

If the server is crash then the system shall display "**The Server is Down**" button.

POST-CONDITIONS

- Administrator can a list view remote PC's devices information
- Administrator can rearrange the displayed list by either the deice name or device status

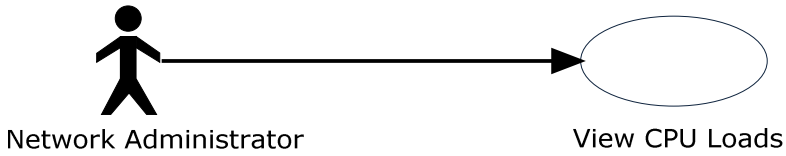
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

USE CASE: View CPU Load (RNMS_01_06)



BRIEF DESCRIPTION

This use case is initiated by the network administrator. This use will not be initiated unless the administrator has a successful log in to the system. This use case enable network's administrator to view monitored PC's CPU load; a chart will be drawn show the remote PC's CPU load for the last 1 hour.

PRE-CONDITIONS

- Administrator must be successfully logged in
- System successfully connected to the remote PC

CHARACTERISTIC OF ACTIVATION

Event driven (Administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the administrator presses on the "CPU Monitor" navigation button in the home page main menu
- If the system successfully connects to the remote PC (using the IP chosen by the administrator) the system shall display remote PC's CPU load Information
- The administrator can view updated information about the remote PC's CPU load details by press the "Refresh" button to re-connect again with the remote PC and get the current CPU status.
- The administrator can press "Save to Archive" button to initiate the **Archive CPU Load Information USE CASE (RNMS_07_06)** by send sending the displayed details to the RNMS database.
- If the system could not connect to the remote PC successfully then the system shall display error message to inform the administrator about what error was happened. (Exception follows **E1)**.
- If the administrator is not logged in successfully then the system should redirect the administrator to the login page.

Alternative Flow

Not Applicable.

Exceptional Flow

E-1: Connection Error (RNMS_01_01_01)

The system shall display a message about what error was happened while trying to connect to the remote PC. The system shall not show the "**Save to Archive**" button.

E-2: Web Server Error (RNMS_01_01_02)

If the server is crash then the system shall display "**The Server is Down**" button.

POST-CONDITIONS

Not applicable

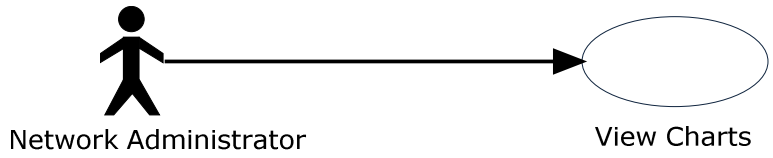
RULE(S)

Not applicable

CONSTRAINT(S)

Not applicable

USE CASE: View Charts (RNMS_01_7)



RIEF DESCRIPTION

This use case is initiated by the network administrator. This use will not be initiated unless the administrator has a successful log in to the system. This use case enable network's administrator to view charts about the managed PCs; including storage usage, CPU loads, and up time (those charts will be created based on the stored information about the managed

PC's in the RNMS database). This use case allows the network administrator to print the displayed charts or save them as PDF files or JPEG files.

PRE-CONDITIONS

- Administrator must be successfully logged in
- System successfully connected to the RNMS database

CHARACTERISTIC OF ACTIVATION

Event driven (Administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the administrator presses on the "Chart" navigation button on the home page main menu
- If the system successfully connects to the RNMS database then the system shall display charts based on the stored information in the RNMS archives. Those charts include; managed PCs' storage usage, CPU loads, and up time (how many hours the system was working).
- The administrator can press "Save" button to initiate the **Archive Charts USE CASE (RNMS_07_07).**
- If the system could not connect to the RNMS database successfully then the system shall display error message to inform the administrator about what error was happened. (Exception follows **E1)**.
- If the administrator is not logged in successfully then the system should redirect the administrator to the login page.

Alternative Flow

Not Applicable.

Exceptional Flow

E-1: Database connection Error (RNMS_01_07_01) The system shall display the message "Database connection Error Please try again, if the Error is still appear s please contact the database server manager". The system will suspend waiting the administrator next action.

POST-CONDITIONS

The administrator will be able to save the displayed charts

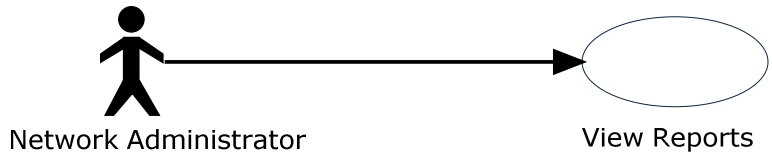
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable.

USE CASE: View Reports (RNMS_01_08)



BRIEF DESCRIPTION

This use case is initiated by the network administrator. This use will not be initiated unless the administrator has a successful log in to the system and the system has a successful connection to the RMNS database. This use case display reports about the managed PCs; total number of the

managed PCs, their location, their Name, and the last connected to the system.

PRE-CONDITIONS

- Administrator must be successfully logged in
- System successfully connected to the RNMS database

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the administrator presses on the "Reports" navigation button on the home page main menu
- If the administrator is logged in and the system successfully connects to the RNMS database then the system shall display reports based on the stored information in the RNMS archives. Those reports include; Number of managed PCs, their name, their location, and last time they connected to system.
- The administrator can press "Save" button to initiate the **Archive Reports USE CASE (RNMS_07_08).**
- If the system could not connect to the RNMS database successfully then the system shall display error message to inform the administrator about what error was happened. (Exception follows **E1)**.
- If the administrator is not logged in then the system should redirect the administrator to the login page

Alternative Flow

Not Applicable.

Exceptional Flow

E-1: Database connection Error (RNMS_01_08_01)

The system shall display the message "Database connection Error Please try again, if the Error is still appear s please contact the database server manager". The system will suspend waiting the administrator next action.

POST-CONDITIONS

The administrator will be able to save the displayed charts

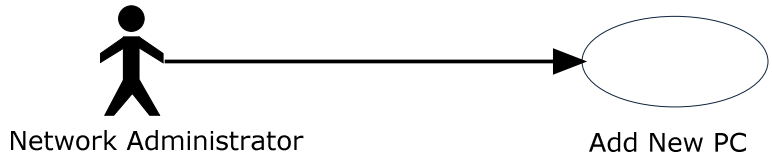
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

USE CASE: Add New PC (RNMS_02_01)



BRIEF DESCRIPTION

The network administrator will initiate this use case to add new PC to the RMNS. This use case will not initiate unless the administrator is logged in successfully to the system. After adding the new PC IP address then the system shall add the new PC to the managed PCs List.

PRE-CONDITIONS

- Administrator must be successfully logged in to the system
- System successfully connected to the RNMS database.

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press “Add Node” button on the main menu
- If the server not responds then the system shall display Error message (Exception flow **E1)**.
- If the system connected to web server successfully the system shall display the add node page
- The administrator type IP address in the IP address textbox, then the press on the “Add Node” button
- The system will check the format of the entered IP address and inform the administrator if the format is not correct
- The system Add the accepted IP format to the “Managed PC Table” in RNMS database
- If the system filed to connect to the RNMS database then Error message should be printed telling the administrator what error was happened (Exception flow **E2**)
- The system will suspend waiting the next action of the administrator

Alternative Flow

Not Applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_02_01_01)

The system shall display the message "the system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator". The system will suspend waiting the next action from the administrator.

E-2: Cannot connect to the Database Server (RNMS_02_01_02)

The system shall display the message "The system filed to connect to the database server". The system will suspend waiting the next action from the administrator.

POST-CONDITIONS

The administrator shall be able to access the new node information using the system

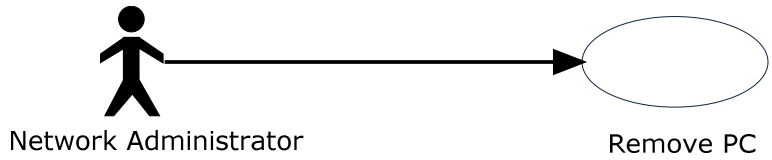
RULE(S)

Not applicable.

CONSTRAINT(S)

The entered IP address should be written in correct format.

USE CASE: Remove PC (RNMS_02_02)



BRIEF DESCRIPTION

The network administrator will initiate this use case to remove PC from the RMNS PC list. This use case will not initiate unless the administrator

is logged in successfully to the system. After removing the PC then the PC should be deleted from the managed PC list as well as from the RNMD database

PRE-CONDITIONS

- Administrator must be successfully logged in to the system
- System successfully connected to the RNMS database

CHARACTERISTIC OF ACTIVATION

Event driven (Administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press “Remove Node” button on the main menu
- If the server not responds then the system shall display Error message (Exception flow **E1)**.
- If the system connected to web server successfully the system shall display “remove node” page, the page will display a list of all the managed PC
- The administrator select the PC IP address from the displayed list
- The administrator press “Remove Node” button
- The system connects to the RNMS database and removes the selected PC from the database. The system shall display a message telling the administrator if removing the selected PC is done successfully
- If the system filed to connect to the RNMS database then Error message should be printed telling the administrator what error was happened (Exception flow **E2**)

- The system will suspend waiting the next action from the administrator

Alternative Flow

Not Applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_02_02_01)

The system shall display the message "The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator". The system will suspend waiting the next action from the administrator

E-2: Cannot connect to the Database Server (RNMS_02_01_02)

The system shall display the message "The system filed to connect to the database server". The system will suspend waiting the next action from the administrator

POST-CONDITIONS

- The system should remove the removed PC from the managed PC

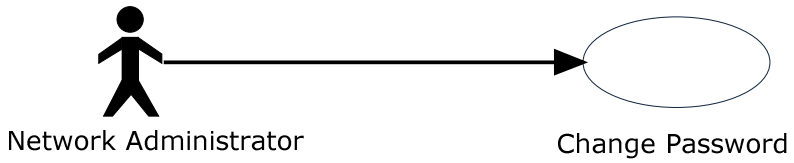
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable.

USE CASE: Change Password (RNMS_03_01)



BRIEF DESCRIPTION

The network administrator will initiate this use case to change his/her RMNS's password. The use case will allow the network administrator to change his/her password and will send an email telling him/her about the new password.

PRE-CONDITIONS

- The administrator must be logged in to the system
- The administrator must verify his log in again (for security reasons)

CHARACTERISTIC OF ACTIVATION

Event driven (administrator Demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press "User Account" button on the main menu
- If the server not responds then the system shall display Error message (Exception flow **E1)**.
- If the system connected to web server successfully the system shall display "User Account" page

- The administrator select change password
- The system ask the administrator to enter his current password, the new password, and verify the new password again
- The administrator enter his/her current password, and the new password, and renter the new password again and press “Submit” button
- If the system successfully connected to the RNMS database then the system shall verify the administrator current password
- If the current password matched then the system should change the password in the RNMS database and then display a message telling the administrator that the password was changed successfully
- If the system filed to connect to the RNMS database then Error message should be printed telling the administrator what error was happened (Exception flow **E2**)
- If the current password not match the administrator password then the system will ask the administrator to enter his password again
- The system will suspend waiting the next action from the administrator

Alternative Flow

Not Applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_02_01_01)

The system shall display the message “The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator”. The system will suspend waiting the next action from the administrator

E-2: Cannot connect to the Database Server (RNMS_02_01_02)

The system shall display the message "The system filed to connect to the database server". The system will suspend waiting the next action from the administrator

POST-CONDITIONS

The new administrator password is set

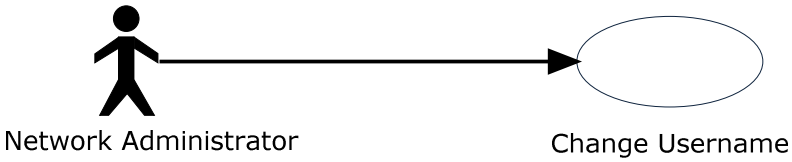
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable.

USE CASE: Change Username (RNMS_03_02)



BRIEF DESCRIPTION

The network administrator will initiate this use case to change his/her RMNS's Username. The use case will allow the network administrator to change his/her Username and will send an email telling him/her about the new changes.

PRE-CONDITIONS

- The administrator must be logged in to the system

- The administrator must verify his log in again (for security reasons)

CHARACTERISTIC OF ACTIVATION

Event driven (Administrator Demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press "User Account" button on the main menu
- If the server does not respond then the system shall display Error message (Exception flow **E1)**.
- If the system connected to web server successfully the system shall display "User Account" page
- The administrator select change Username
- The system ask the administrator to enter his current password, the new username, and verify the new username again
- The administrator enter his/her current password, and the new Username, and renter the new Username again and press "Submit" button
- If the system successfully connected to the RNMS database then the system shall verify the administrator current password
- If the current password matched then the system should change the username in the RNMS database and then display a message telling the administrator that the username was changed successfully

- If the system filed to connect to the RNMS database then Error message should be printed telling the administrator what error was happened (Exception flow **E2**)
- If the current password not match the administrator password then the system will ask the administrator to enter his password again
- The system will suspend waiting the next action from the administrator

Alternative Flow

Not Applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_02_02_01)

The system shall display the message "The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator". The system will suspend waiting the next action from the administrator

E-2: Cannot connect to the Database Server (RNMS_02_02_02)

The system shall display the message "The system filed to connect to the database server". The system will suspend waiting the next action from the administrator

POST-CONDITIONS

- New administrator username is adopted

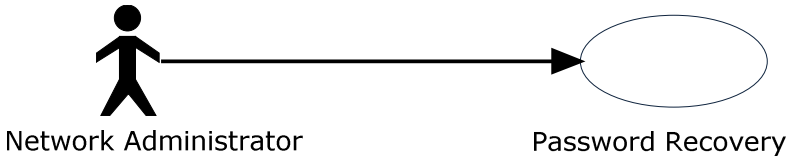
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable.

USE CASE: Password Recovery (RNMS_03_03)



BRIEF DESCRIPTION

The network administrator will initiate this use case to recover his/her RMNS's Password (in case he/she forget his/her password). The use case will send an email to the administrator's email (the administrator email stored in the database) telling him/her the current password and ask him/her to change the password the next time he/she log in to the system (for security reasons)

PRE-CONDITIONS

Not applicable

CHARACTERISTIC OF ACTIVATION

Event driven (administrator Demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press "User Account" button on the main menu

- If the server does not respond then the system shall display Error message (Exception flow **E1)**.
- If the system connected to web server successfully the system shall display "User Account" page
- The administrator select Recovery password option
- The system ask the administrator to enter his Email (the email will be match with the administrator contact in the RNMS database)
- The administrator press "Submit" button
- If the system successfully connected to the RNMS database then the system shall verify the administrator email
- If the email matched then the system should send an email to the administrator's email telling him/her the current password
- If the system filed to connect to the RNMS database then Error message should be printed telling the administrator what error was happened (Exception flow **E2**)
- If the entered email not match the administrator email then the system will ask the administrator to reenter his email again
- The system will suspend waiting the next action from the administrator

Alternative Flow

Not Applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_02_02_01)

The system shall display the message "The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server

administrator". The system will suspend waiting the next action from the administrator

E-2: Cannot connect to the Database Server (RNMS_02_02_02)

The system shall display the message "The system filed to connect to the database server". The system will suspend waiting the next action from the administrator

POST-CONDITIONS

- The Manager will receive an email with his/her password

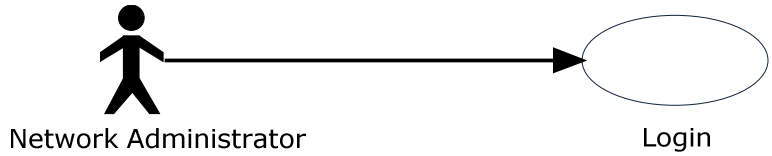
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

USE CASE: Login (RNMS_04)



BRIEF DESCRIPTION

This use case is initiated automatically when the administrator requests the RNMS home page, or when the administrator request any other system function and he is status is "logged out". Also this use case should initiated when the administrator request the "user account" page. If the administrator is successfully logged in to the system then the system should grant access to the administrator to all the system functions. The

login date and time should stored in the system database for archiving purposes.

PRE-CONDITIONS

- The system should successfully connected to the web server
- The system should successfully connected to the database server

CHARACTERISTIC OF ACTIVATION

Event driven (Home page loaded Demand) and the administrator status is "logged out"

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator request the RNMS home page
- If the server does not respond then the system shall display Error message (Exception flow **E1)**.
- If the system connected to web server successfully the system shall display "Login" page
- The administrator enter his/her username and password then press "Login" button
- If the system successfully connected to the RNMS database then the system shall verify the administrator username and password
- If the username and password matched then the system should grant the administrator the authority to login to the RNMS system and archive the login time and date to the "logs archive"

- If the system filed to connect to the RNMS database then Error message should be printed telling the administrator what error was happened (Exception flow **E2**)
- If the entered username and password did not match the administrator username and password then the system will ask the administrator to re-enter the username and password again
- The system will suspend waiting the next action from the administrator

Alternative Flow

Not applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_04_01)

The system shall display the message "The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator". The system will suspend waiting the next action from the administrator

E-2: Cannot connect to the Database Server (RNMS_04_02)

The system shall display the message "The system filed to connect to the database server". The system will suspend waiting the next action from the administrator

POST-CONDITIONS

- The system will grant access authority to the administrator
- The login time and date should be archived to the system "log table"

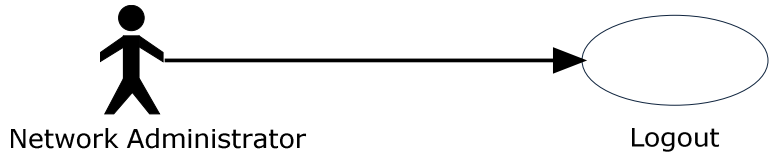
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

USE CASE: Logout (RNMS_05)



BRIEF DESCRIPTION

This use case is initiated when the administrator press the "Logout" button. If the administrator is successfully logged out from the system then the access grant will taken from the administrator. the administrator have to re-login again to access the system.

PRE-CONDITIONS

- The system should successfully connected to the web server
- The system should successfully connected to the database server

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press the "Logout" button

- If the server does not respond then the system shall display Error message (Exception flow **E1)**.
- The system will change the administrator status to "Logout"
- If the system successfully connected to the RNMS database then the system shall archive the logout time and date to the system log archive
- The system will suspend redirect the administrator to the "Login page" and suspend waiting the administrator next action

Alternative Flow

Not applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_05_01)

The system shall display the message "The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator". The system will suspend waiting the next action from the administrator

POST-CONDITIONS

- The system will taken the grant access authority from the administrator and change his status to "logout"
- The logout time and date should be archived to the system "log table"

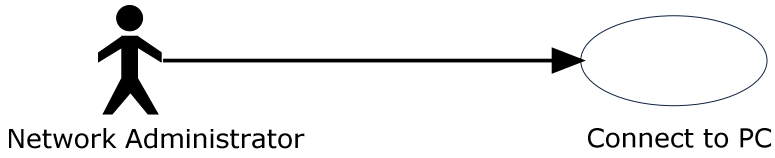
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

USE CASE: Connect to PC (RNMS_06)



BRIEF DESCRIPTION

This use case is initiated when the administrator press the "Connect" button. The administrator must be logged in order to connect to a PC. If the system successfully connected to the remote PC (using the IP address which selected by the administrator first) then the can view remote PC, storage information, running processes information, Software details, devices details and can view some charts about the remote PC performance history.

PRE-CONDITIONS

- The system should successfully connected to the web server
- The administrator must be logged in

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press the "connect" button
- If the web server does not respond then the system shall display Error message (Exception flow **E1)**.
- The system will try to connect to the remote PC (the one with the selected IP address from the computer s list)
- If the system successfully connected to remote PC then the system should redirect the administrator to the "General Information"
- If the system is failed to connect to the selected PC then the system should print a message telling the administrator what error was occur during the connection (**E2**)

Alternative Flow

Not applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_06_01)

The system shall display the message "The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator". The system will suspend waiting the next action from the administrator

E-2: The system failed to connect to the remote PC (RNMS_06_02)

If the system failed to connect to the remote PC then the system should print an error message telling the administrator what error

was occur during the connection. The system will suspend waiting the next action from the administrator

POST-CONDITIONS

- The system will get the current status of the remote PC; general information, devices information, storage information, software information, running processes information, and the CPU load details.

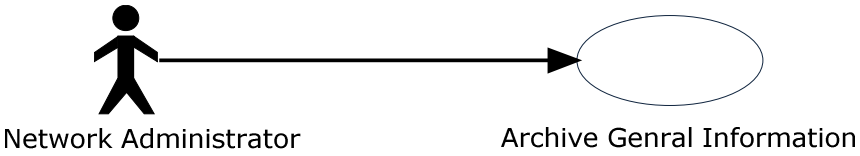
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

USE CASE: Archive General Information (RNMS_07_01)



BRIEF DESCRIPTION

This use case is initiated when the administrator press the "Save to Archive" button on the "General Information" page. This use case will be enabled if the system successfully connected to the selected remote PC. Also, the administrator must be logged in order to access this service. The system then will copy the remote PC general information to the RNMS database.

PRE-CONDITIONS

- The system must be successfully connected to the web server
- The system must be successfully connected to the selected remote PC
- The administrator must be logged in

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press the "Save to Archive" button on the "General Information" page
- If the web server does not respond then the system shall display Error message (Exception flow **E1)**.
- If the system successfully connected to the RNMS database then the system should insert the general information into the "general" table in the RNMS database
- If the system failed to connected to the RNMS database then the system should display error message (**E2**)
- If the system successfully inserted the data then the system should print a message telling the administrator that the insert was done successfully
- The system will suspend waiting the next action from the administrator

Alternative Flow

Not applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_07_01_01)

The system shall display the message “The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator”. The system will suspend waiting the next action from the administrator

E-2: The system failed to connect to the RNMS database (RNMS_07_01_02)

If the system failed to connect to RNMS database then the system should print “The system failed to connect to the RNMS database, please try again. If the problem still occurs then you have to contact the database server’s administrator”. The system will wait next administrator action

POST-CONDITIONS

- The system should insert the displayed information into the general information table into the RNMS database

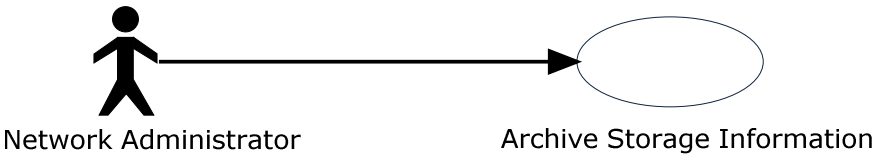
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

USE CASE: Archive Storage Information (RNMS_07_02)



BRIEF DESCRIPTION

This use case is initiated when the administrator press the "Save to Archive" button on the "Storage" page. This use case will be enabled if the system was successfully connected to the selected remote PC. Also, the administrator must be logged in order to access this service. The system then will copy the remote PC storage information to the RNMS database.

PRE-CONDITIONS

- The system should successfully connected to the web server
- The system should successfully connected to the selected remote PC
- The administrator must be logged in

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press the "Save to Archive" button on the "Storage" page
- If the web server does not respond then the system shall display Error message (Exception flow **E1)**.

- If the system successfully connected to the RNMS database then the system should insert the storage information into the storage information table in the RNMS database
- If the system is failed to connected to the RNMS database then the system should display error message (**E2**)
- If the system successfully inserted the data then the system should print a message telling the administrator that the inserted done successfully
- The system will suspend waiting the next action from the administrator

Alternative Flow

Not applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_07_02_01)

The system shall display the message "The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator". The system will suspend waiting the next action from the administrator

E-2: The system failed to connect to the RNMS database (RNMS_07_02_02)

If the system failed to connect to RNMS database then the system should print "The system failed to connect to the RNMS database, please try again. If the problem still occurs then you have to

contact the database server's administrator". The system will wait next administrator action

POST-CONDITIONS

- The system should insert the displayed device information into the device information table into the RNMS database

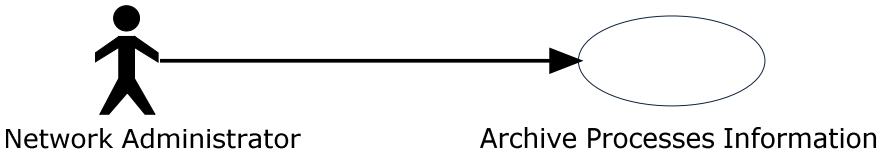
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

USE CASE: Archive Running Processes Information (RNMS_07_03)



BRIEF DESCRIPTION

This use case is initiated when the administrator press the "Save to Archive" button on the "Running Processes" page. This use case will be enabled if the system was successfully connected to the selected remote PC. Also, the administrator must be logged in order to access this service. The system then will copy the remote PC running processes information to the RNMS database.

PRE-CONDITIONS

- The system should successfully connected to the web server
- The system should successfully connected to the selected remote PC
- The administrator must be logged in

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press the "Save to Archive" button on the "Running Processes" page
- If the web server does not respond then the system shall display Error message (Exception flow **E1)**.
- If the system successfully connected to the RNMS database then the system should insert the Processes information into the "Processes" table in the RNMS database
- If the system failed to connected to the RNMS database then the system should display error message (Exception flow**E2**)
- If the system successfully inserted the data then the system should print a message telling the administrator that the inserted done successfully
- The system will suspend waiting the next action from the administrator

Alternative Flow

Not applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_07_03_01)

The system shall display the message “The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator”. The system will suspend waiting the next action from the administrator

E-2: The system failed to connect to the RNMS database (RNMS_07_03_02)

If the system failed to connect to RNMS database then the system should print “The system failed to connect to the RNMS database, please try again. If the problem still occurs then you have to contact the database server’s administrator”. The system will wait next administrator action

POST-CONDITIONS

- The system should insert the displayed running processes information into the “Processes” table into the RNMS database

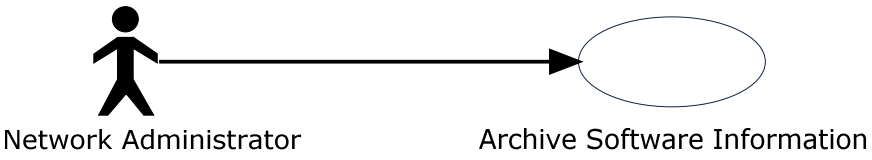
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

USE CASE: Archive Software Information (RNMS_07_04)



BRIEF DESCRIPTION

This use case is initiated when the administrator press the "Save to Archive" button on the "Software" page. This use case will be enabled if the system was successfully connected to the selected remote PC. Also, the administrator must be logged in order to access this service. The system then will copy the remote PC software information to the RNMS database.

PRE-CONDITIONS

- The must be successfully connected to the web server
- The must be successfully connected to the selected remote PC
- The administrator must be logged in

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press the "Save to Archive" button on the "Software" page
- If the web server does not respond then the system shall display Error message (Exception flow **E1)**.

- If the system successfully connected to the RNMS database then the system should insert the software information into the "Software" table in the RNMS database
- If the system is failed to connected to the RNMS database then the system should display error message (**E2**)
- If the system successfully inserted the data then the system should print a message telling the administrator that the inserted done successfully
- The system will suspend waiting the next action from the administrator

Alternative Flow

Not applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_07_04_01)

The system shall display the message "The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator". The system will suspend waiting the next action from the administrator

E-2: The system failed to connect to the RNMS database (RNMS_07_04_02)

If the system failed to connect to RNMS database then the system should print "The system failed to connect to the RNMS database, please try again. If the problem still occurs then you have to

contact the database server's administrator". The system will wait next administrator action

POST-CONDITIONS

- The system should insert the displayed software information into the "Software" table into the RNMS database

RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

USE CASE: Archive Devices Information (RNMS_07_05)

BRIEF DESCRIPTION

This use case is initiated when the administrator press the "Save to Archive" button on the "Devices" page. This use case will be enabled if the system was successfully connected to the selected remote PC. Also, the administrator must be logged in order to access this service. The system then will copy the remote PC devices information to the RNMS database.

PRE-CONDITIONS

- The system must be successfully connected to the web server
- The system must be successfully connected to the selected remote PC
- The administrator must be logged in

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press the "Save to Archive" button on the "Devices" page
- If the web server does not respond then the system shall display Error message (Exception flow **E1)**.
- If the system successfully connected to the RNMS database then the system should insert the devices information into the "Devices" table in the RNMS database
- If the system is failed to connected to the RNMS database then the system should display error message (**E2**)
- If the system successfully inserted the data then the system should print a message telling the administrator that the inserted done successfully
- The system will suspend waiting the next action from the administrator

Alternative Flow

Not applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_07_01_01)

The system shall display the message "The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator". The system will suspend waiting the next action from the administrator

E-2: The system failed to connect to the RNMS database (RNMS_07_01_02)

If the system failed to connect to RNMS database then the system should print "The system failed to connect to the RNMS database, please try again. If the problem still occurs then you have to contact the database server's administrator". The system will wait next administrator action

POST-CONDITIONS

- The system should insert the displayed device information into the "Device"table into the RNMS database

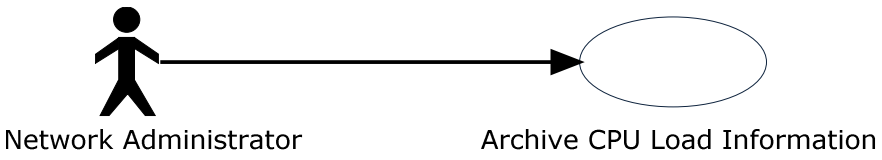
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

USE CASE: Archive CPU Load Information (RNMS_07_06)



BRIEF DESCRIPTION

This use case is initiated when the administrator press the "Save to Archive" button on the "CPU Monitor" page. This use case will be enabled if the system was successfully connected to the selected remote PC. Also, the administrator must be logged in order to access this service. The system then will copy the remote PC CPU loads information to the RNMS database.

PRE-CONDITIONS

- The system must be successfully connected to the web server
- The system must be successfully connected to the selected remote PC
- The administrator must be logged in

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press the "Save to Archive" button on the "CPU Monitor" page
- If the web server does not respond then the system shall display Error message (Exception flow **E1)**.
- If the system successfully connected to the RNMS database then the system should insert the devices information into the "CPU Load" table in the RNMS database
- If the system is failed to connected to the RNMS database then the system should display error message (**E2**)
- If the system successfully inserted the data then the system should print a message telling the administrator that the inserted done successfully
- The system will suspend waiting the next action from the administrator

Alternative Flow

Not applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_07_06_01)

The system shall display the message "The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator". The system will suspend waiting the next action from the administrator

E-2: The system failed to connect to the RNMS database (RNMS_07_06_02)

If the system failed to connect to RNMS database then the system should print "The system failed to connect to the RNMS database, please try again. If the problem still occurs then you have to contact the database server's administrator". The system will wait next administrator action

POST-CONDITIONS

- The system should insert the displayed CPU load information into the "CPU Load" table into the RNMS database

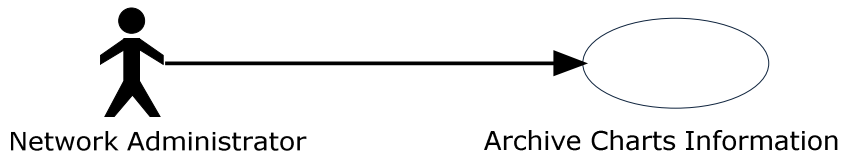
RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

USE CASE: Archive CPU Load Information (RNMS_07_07)



BRIEF DESCRIPTION

This use case is initiated when the administrator press the "Save to Archive" button on the "Charts" page. This use case will be enabled if the system was successfully connected to the selected remote PC. Also, the

administrator must be logged in order to access this service. The system then will inset the remote PC Charts to the RNMS database.

PRE-CONDITIONS

- The system must be successfully connected to the web server
- The system must be successfully connected to the selected remote PC
- The administrator must be logged in

CHARACTERISTIC OF ACTIVATION

Event driven (administrator demand)

FLOW OF EVENTS

Basic Flow

- This use case begins when the network administrator press the "Save to Archive" button on the "Charts" page
- If the web server does not respond then the system shall display Error message (Exception flow **E1)**.
- If the system successfully connected to the RNMS database then the system should insert the charts into the "Charts" table in the RNMS database (the charts will be stored as images into the database)
- If the system is failed to connected to the RNMS database then the system should display error message (**E2**)
- If the system successfully inserted the data then the system should print a message telling the administrator that the inserted done successfully
- The system will suspend waiting the next action from the administrator

Alternative Flow

Not applicable.

Exceptional Flow

E-1: Cannot connect to the Web Server (RNMS_07_06_01)

The system shall display the message "The system filed to connect to the web server. Check your internet connection and try again. If the problem still appears then contact the web server administrator". The system will suspend waiting the next action from the administrator

E-2: The system failed to connect to the RNMS database (RNMS_07_07_02)

If the system failed to connect to RNMS database then the system should print "The system failed to connect to the RNMS database, please try again. If the problem still occurs then you have to contact the database server's administrator". The system will wait next administrator action

POST-CONDITIONS

- The system should insert the displayed charts into the "Charts" table into the RNMS database

RULE(S)

Not applicable.

CONSTRAINT(S)

Not applicable

APPENDIX D
RNMS PAGES SCREEN SHOTS

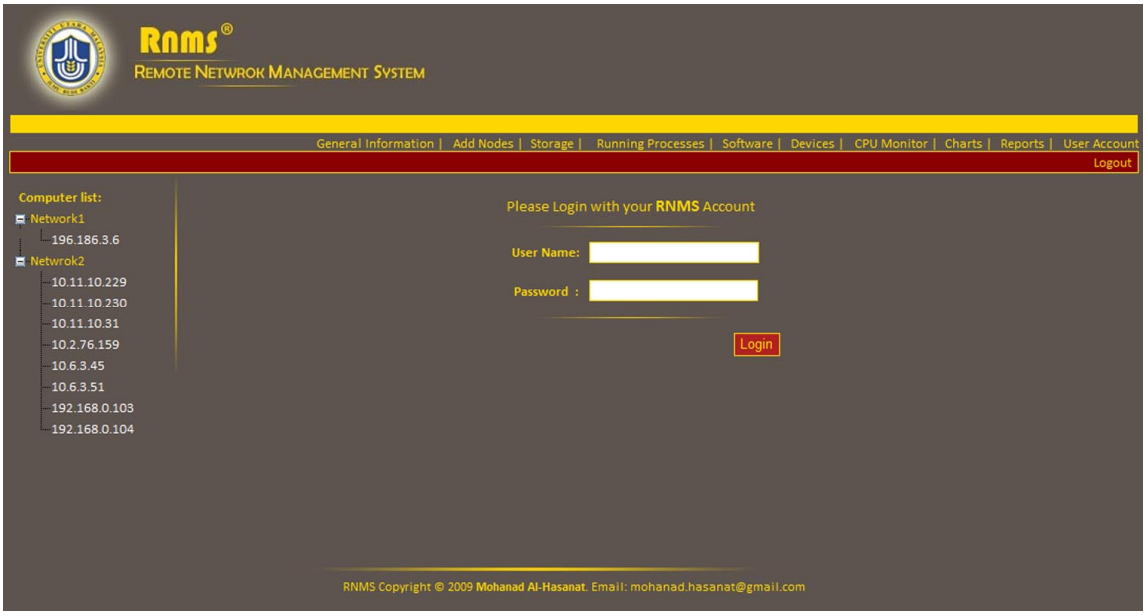


Figure1: RNMS Login Page

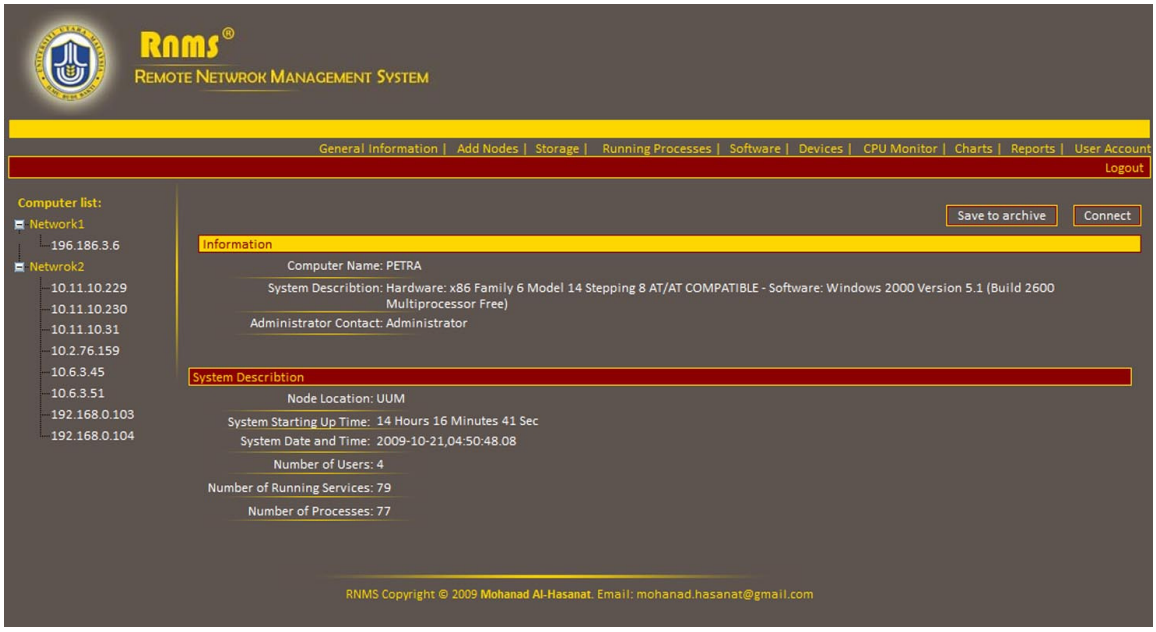


Figure 2: RNMS Home Page

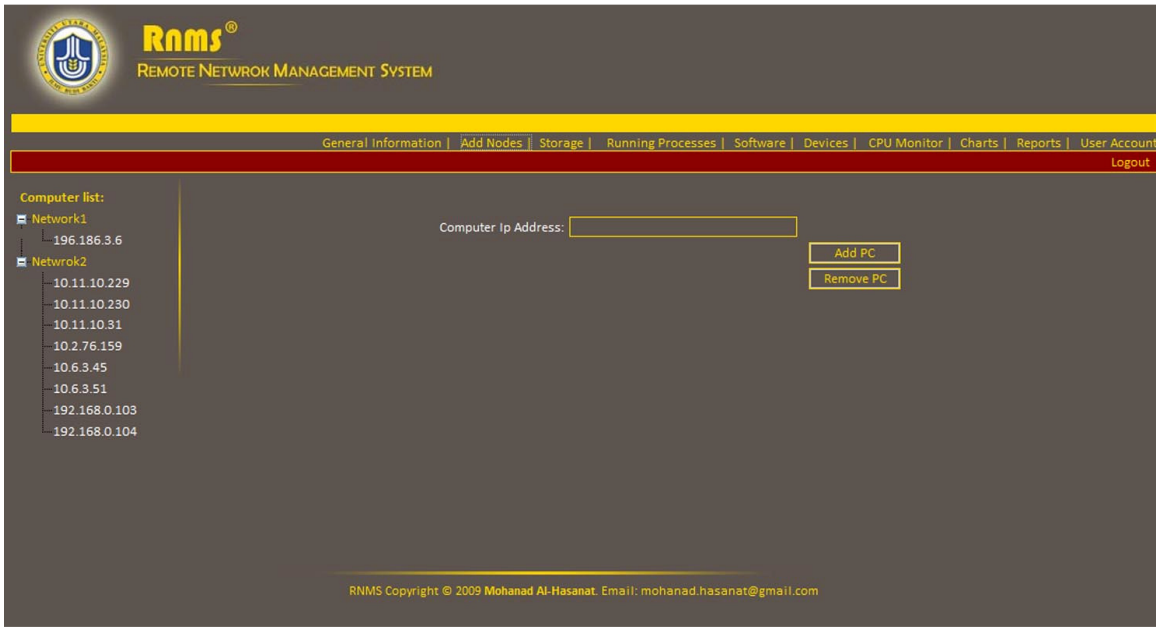


Figure3: Add\Remove Node

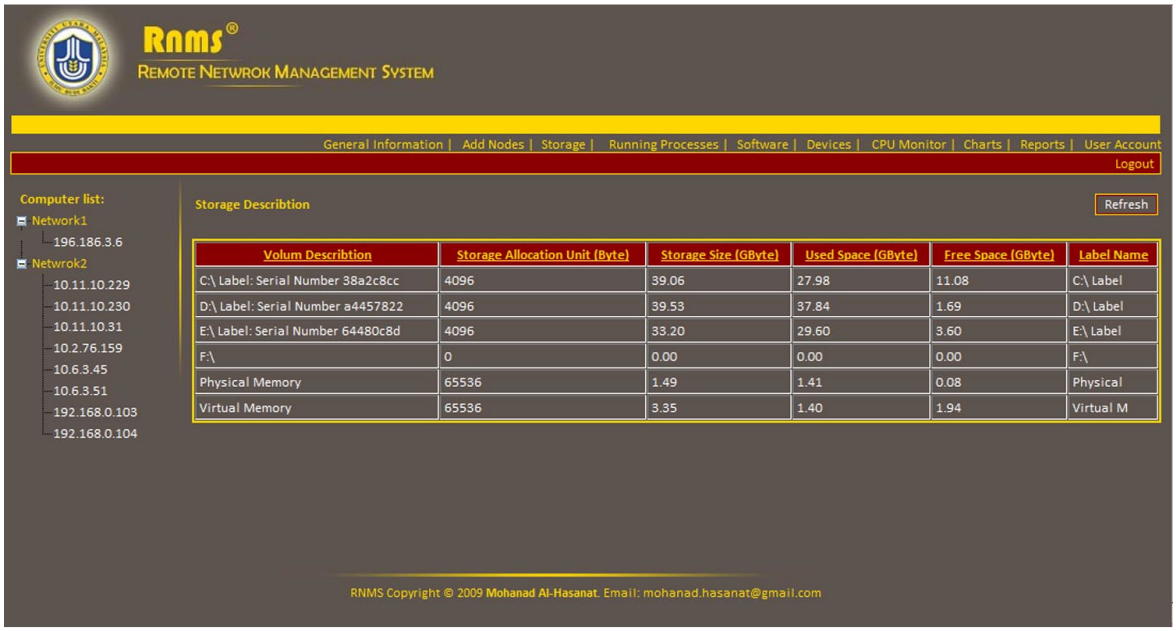


Figure4: View Remote PC Storage Details

Figure5: Remote PC's processes details

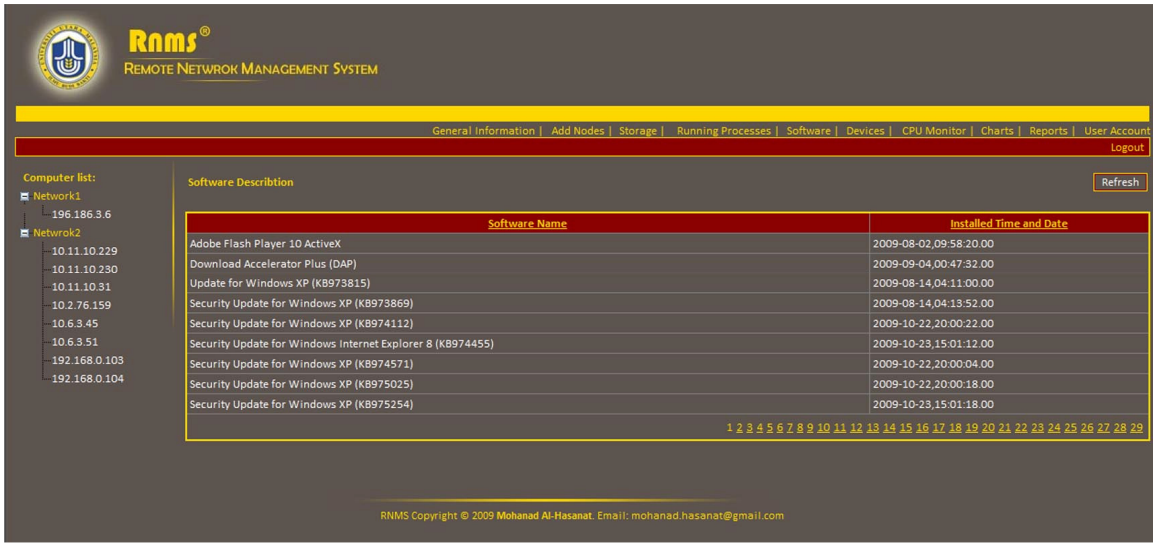


Figure6: Remote PC's Software details

Figure7: Remote PC's devices details

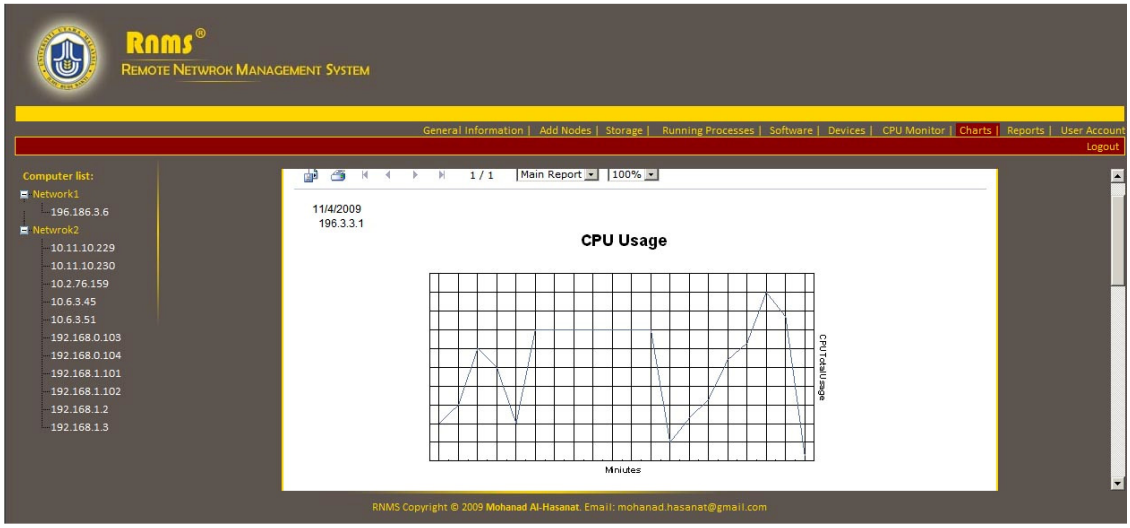


Figure8: Remote CPU Monitoring Chart

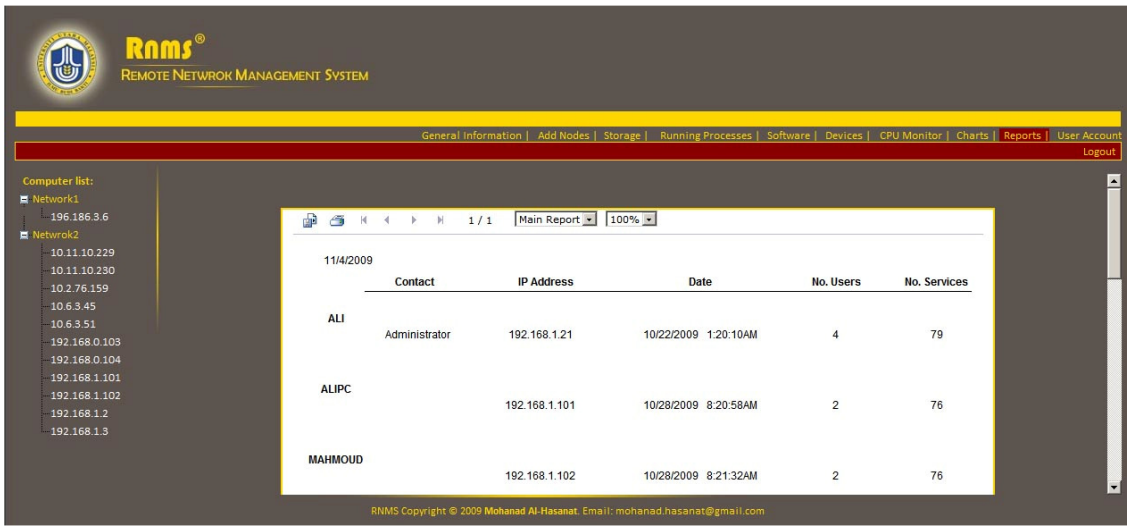


Figure9: Monitored PCs report

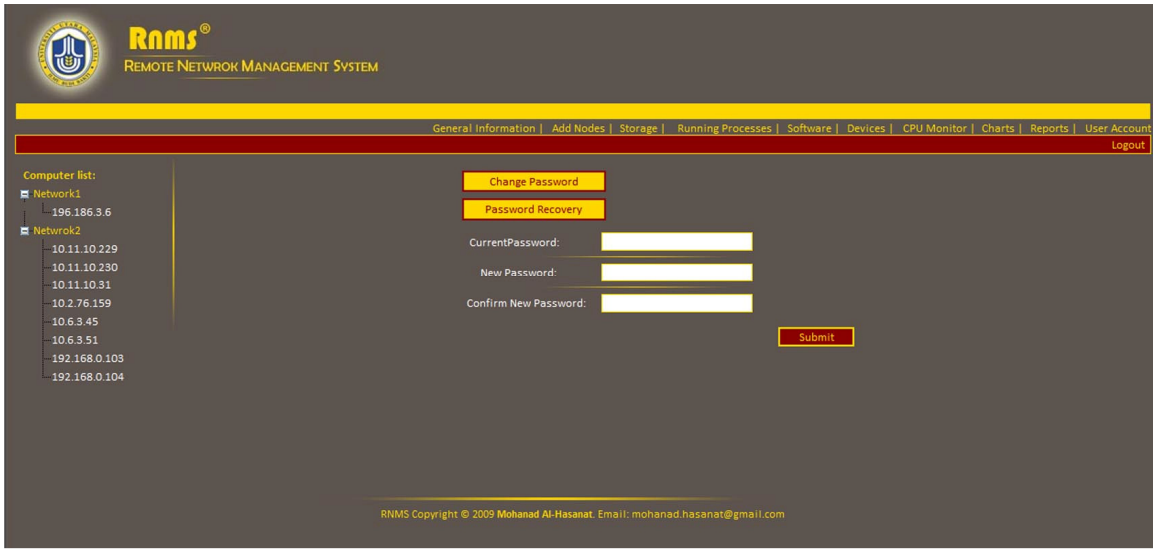


Figure10: Remote PC's User Account Page

APPENDIX E

Technology Acceptance Model Questionnaire

Remote Network Management System (RNMS)

This survey aims to evaluate the Remote Network Management System (RNMS) by testing your acceptance after navigating the proposed system. Kindly fill out the following;

Name: ……. Position: ……

Academic background:

1. Diploma 2. Bachelor 3. Master 4. Doctoral

For each item identified below, circle the number to the right that best fits your judgment of it is quality (1= Strongly Disagree, 2= Disagree, 3= Somewhat Disagree, 4=Somewhat Agree, 5= Agree, 6=Strongly Agree)

ID	Description of survey item	Scale					
Preserve Usefulness (PU)							
1.	Using the RNMS system will enable networks managers to accomplish their tasks more quickly	1	2	3	4	5	6
2.	Using the RNMS improves networks managers performance	1	2	3	4	5	6
3.	Using RNMS will increase networks managers productivity	1	2	3	4	5	6
4.	Using RNMS enhances networks managers effectiveness in their jobs	1	2	3	4	5	6
Preserve Ease of Use (PEU)							
5.	My integration with the RNMS is clear and	1	2	3	4	5	6

	understandable						
6.	Interacting with the RNMS does not require a lot of my metal effort	1	2	3	4	5	6
7.	I find the RNMS easy to use	1	2	3	4	5	6
8.	I find the RNMS easy to get what I want	1	2	3	4	5	6

9. After testing the system, what other functions should be included to enhance the RNMS's ability?

……

……

……..

10. Comments /Suggestions:

……

……

……..

Thank you for taking the time to help me with my little research

APPENDIX F

Descriptive statistics of the questioner's data analysis

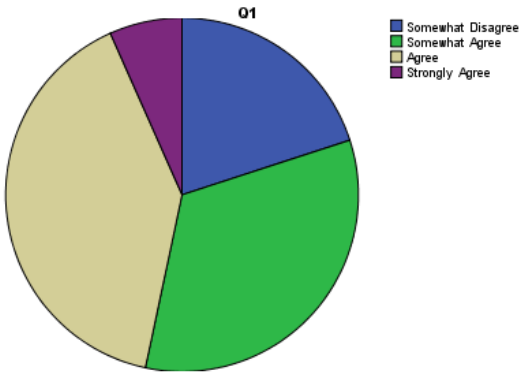
Statistics

		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
N	Valid	15	15	15	15	15	15	15	15
	Missing	0	0	0	0	0	0	0	0
Mean		4.33	4.53	4.20	4.33	4.47	4.60	4.47	4.60
Median		4.00	5.00	4.00	4.00	4.00	4.00	4.00	4.00
Mode		5	5	4	5	4	4	4	4
Minimum		3	3	3	3	4	4	4	4
Maximum		6	6	6	6	6	6	6	6
Percentiles	25	4.00	4.00	3.00	3.00	4.00	4.00	4.00	4.00
	50	4.00	5.00	4.00	4.00	4.00	4.00	4.00	4.00
	75	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00

Frequency Tables:

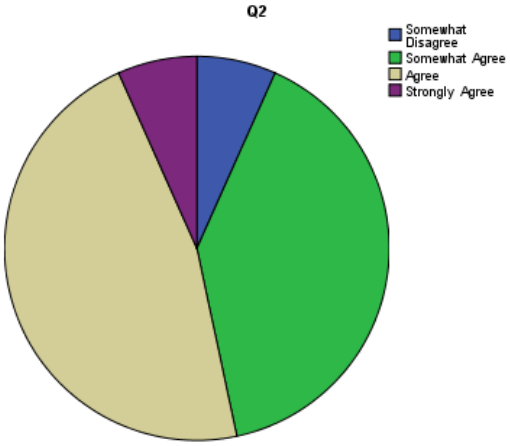
Q1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Disagree	3	20.0	20.0	20.0
	Somewhat Agree	5	33.3	33.3	53.3
	Agree	6	40.0	40.0	93.3
	Strongly Agree	1	6.7	6.7	100.0
	Total	15	100.0	100.0	



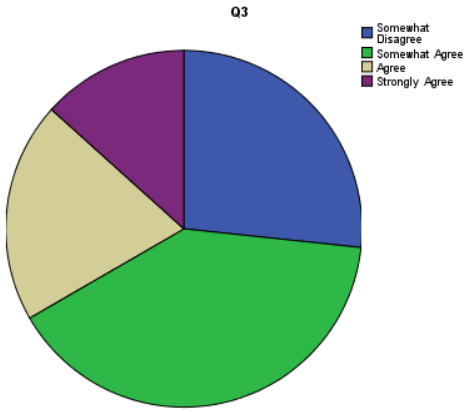
Q2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Disagree	1	6.7	6.7	6.7
	Somewhat Agree	6	40.0	40.0	46.7
	Agree	7	46.7	46.7	93.3
	Strongly Agree	1	6.7	6.7	100.0
	Total	15	100.0	100.0	



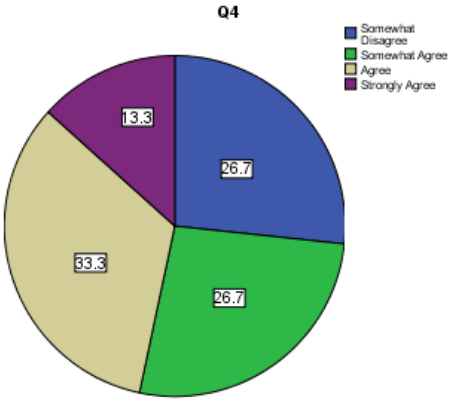
Q3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Disagree	4	26.7	26.7	26.7
	Somewhat Agree	6	40.0	40.0	66.7
	Agree	3	20.0	20.0	86.7
	Strongly Agree	2	13.3	13.3	100.0
	Total	15	100.0	100.0	



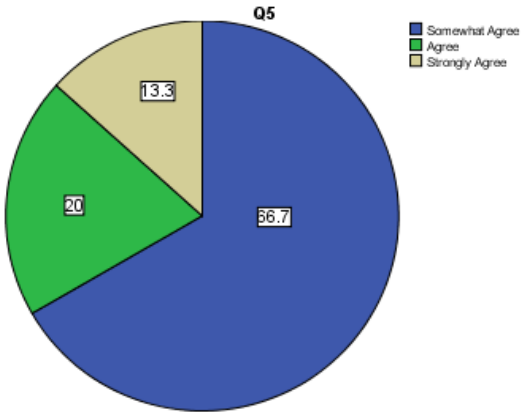
Q4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Disagree	4	26.7	26.7	26.7
	Somewhat Agree	4	26.7	26.7	53.3
	Agree	5	33.3	33.3	86.7
	Strongly Agree	2	13.3	13.3	100.0
	Total	15	100.0	100.0	



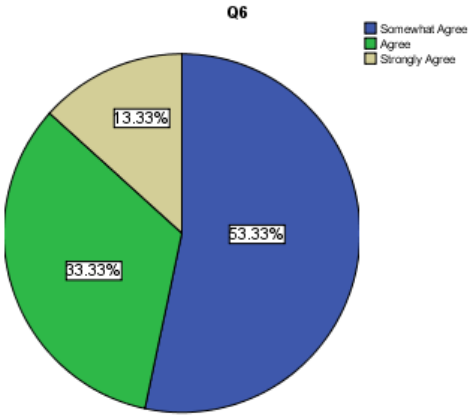
Q5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Agree	10	66.7	66.7	66.7
	Agree	3	20.0	20.0	86.7
	Strongly Agree	2	13.3	13.3	100.0
	Total	15	100.0	100.0	



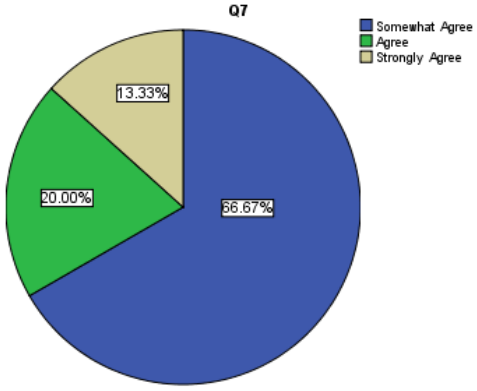
Q6

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Agree	10	66.7	66.7	66.7
	Agree	3	20.0	20.0	86.7
	Strongly Agree	2	13.3	13.3	100.0
	Total	15	100.0	100.0	



Q7

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Agree	10	66.7	66.7	66.7
	Agree	3	20.0	20.0	86.7
	Strongly Agree	2	13.3	13.3	100.0
	Total	15	100.0	100.0	



Q8

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Agree	8	53.3	53.3	53.3
	Agree	5	33.3	33.3	86.7
	Strongly Agree	2	13.3	13.3	100.0
	Total	15	100.0	100.0