AN INNOVATIVE SYSTEM TO MONITOR E-MAIL SYSTEMS ENVIRONMENTS USING ACTIVE MONITORING

by

HUSSEIN ABDELRAHMAN HUSSEIN ALBAZAR

Thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

June 2010

ACKNOWLEDGMENTS

This piece of work would have never been accomplished without the blessings from Allah the Almighty. You have given me the inner power which have been always inspiring, guiding and accompanying me through thick and thin. You have made my life more meaningful. May your name be exalted, honored, and glorified.

First and foremost I would like to offer my deep and sincere gratitude to my supervisor, Professor Dr. Sureswaran Ramadass, Director of the National Advanced IPv6 Centre (NAv6), University Sains Malaysia. His wide knowledge and enthusiasm have been of great value for me as I look upon him as my role model. His understanding, encouragement and personal guidance have provided me a good basis for my research and my thesis writing. One simply could not wish for a better or friendlier supervisor.

I would like to express my sincere appreciation to my co-supervisor, Dr. Omar Amer Abouabdalla, for his encouragement, guidance, advices and motivation.

I also wish to thank all staffs of NAv6 Centre; School of Computer Sciences, USM and Institute for Graduate Studies (IPS), USM for helping me in many ways during my research and thesis writing. The financial support of the Universiti Sains Malaysia through the USM fellowship scheme is gratefully acknowledged.

I owe my loving thanks to my parents, mother and father, and my wife, Hala. Without their encouragement and understanding it would have been impossible for me to finish my PhD. My special gratitude to my brothers, my sisters and their

families for their loving support. All these people have made me own a happy family in Jordan.

I would also like to thank all people who have helped and inspired me during my doctoral study. I especially want to thank my friends Mohammed Al-Majali, Adnan Hanif, and my lab mates at the NAv6 Centre. You all have made my stay in Malaysia a meaningful and memorable one.

Thank you!

Hussein Abdelrahman Albazar

Penang, Malaysia. June 2010.

TABLE OF CONTENTS

CHAPTER 4: ACTIVE E-MAIL MONITORING SYSTEM IMPLENITATION

CHAPTER 5: ACTIVE E-MAIL MONITORING SYSTEM TESTING AND RESULTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AEMS	Active E-mail Monitoring System
ARPANET	Advanced Research Project Agency Network
CNAME	Canonical name
DDA	Delayed Delivery Agent
DEM	Decentralized Electronic Mail
DHT	Distributed Hash Table
DNS	Domain Name System
ESMTP	Extension Simple Mail Transfer Protocol
ESP	Email Service Provider
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IMAP	Internet Message Access Protocol
ISP	Internet Services Provider
ITA	International Trade Administrator
MAs	Mobile Agents
MDA	Mail Delivery Agent
MH	Mail Handles
MIME	Multipurpose Internet Mail Extensions
MMDF	Multi-Purpose Memo Distribution Facility
MRAP	Message Resource Allocation Policy
MSG	Message text

MSN	Message Sending Notification
MSP	Message Scheduling Policy
MTA	Message Transport Agent
MTA	Mail Transfer Agent
MTP	Mail Transfer Protocol
MUA	Mail User Agent
MX	Mail exchange
PGP	Pretty Good Privacy
POP	Post Office Protocol
SAN	Storage Area Network
SLA	Service Level Agreement
SLAP	Service Level Agreement Policy
SMTP	Simple Message Transfer Protocol
SOA	Star of Authority
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TTL	Time To Live
UA	User Agent
URL	Unified Recourse Locater

SISTEM INOVATIF UNTUK MEMANTAU PERSEKITARAN SISTEM E-MEL DENGAN MENGGUNAKAN PEMANTAUAN AKTIF

ABSTRAK

Sehingga kini, Sistem E-mail amat penting dalam memenuhi setiap keperluan dalam pelbagai bidang kehidupan seperti pendidikan, perdagangan, pemasaran, komersial and pelbagai bidang perniagaan termasuk komunikasi peribadi melalui Internet. Oleh itu, berjuta-juta mesej E-mail dipertukarkan pada setiap hari di seluruh dunia. Namun keperluan untuk mesej E-mail yang dihantar menerusi Sistem E-mail ini terhalang dari segi kegagalan beberapa perkara tertentu dan memerlukan pemantauan yang tersusun. Prinsip utama kajian ini ialah untuk memperkenalkan Sistem Pemantauan E-mail yang boleh memantau and mengesan kegagalan tersebut.

Sistem yang dicadangkan ialah Sistem Aktif Pemantauan E-mail (Active E-mail Monitoring System, AEMS), yang dibangunkan untuk memantau and mengesan kegagalan perkhidmatan Sistem E-mail di bawah setiap platform Sistem E-mail. AEMS mengandungi satu susunan algoritma pemantauan berdasarkan pemantauan aktif yang berupaya untuk memantau 3 jenis komponen Sistem E-mail utama (E-mail server, DNS server, E-mail gateway), fungsi Sistem E-mail dan perkhidmatan yang tersedia.

Komponen – komponen ini (E-mail server, DNS server, E-mail gateway) bergabung bersama untuk menyediakan perkhidmatan bagi Sistem E-mail dalam penghantaran dan penerimaan mesej E-mail melalui Internet. Kesimpulannya, berdasarkan hasil kajian yang dibuat, AEMS telah terbukti berupaya dalam

memantau komponen – komponen Sistem E-mail (E-mail server, DNS server, E-mail gateway) dan mengesan sebarang kegagalan berkaitan dengan komponen dan meyediakan asas bagi teknik Sistem Pemantauan E-mail. AEMS terdiri daripada susunan algoritma pemantauan, setiap satu menyediakan hasil percubaan dan ianya kemudian disimpan dalam sistem pengkalan data untuk menghasilkan perilaku pengguna bagi komponen pemantauan tersebut. Sistem AEMS juga berupaya untuk memberi amaran kepada pentadbir rangkaian mengenai kegagalan perkhidmatan sekiranya server E-mail mempunyai sebarang masalah atau berfungsi tanpa sebarang keperluan khas atau keadaan. AEMS dibangunkan dengan tujuan untuk memantau Sistem E-mail yang banyak dalam realiti persekitaran kerja dan juga hasil pemantauan membuktikan keupayaannya untuk mengesan masalah fungsi perkhidmatan.

AN INNOVATIVE SYSTEM TO MONITOR E-MAIL SYSTEMS ENVIRONMENTS USING ACTIVE MONITORING

ABSTRACT

In recent times, E-mail systems are essential in fulfilling all correspondences in various fields of our lives such as the education, trading, marketing, commerce and other businesses as well as personal communications via the Internet. Therefore, millions of E-mail messages are exchanged on a daily basis all around the world. The need for these E-mail messages to be delivered is hindered by certain failures within the E-mail systems and requires proper monitoring. Therefore, the principal aim of this research was to introduce an E-mail monitoring system which is able to monitor and detect those failures.

The system proposed is an Active E-mail Monitoring System (AEMS), designed to monitor and detect E-mail system services failure under any E-mail system platform. AEMS consists of a set of monitoring algorithms based on the active monitoring, which are capable of monitoring the three major E-mail system components (E-mail server, DNS server, E-mail gateway), E-mail system functionality and services availability.

These components (E-mail server, DNS System, E-mail gateway) are working together to provide E-mail system services of sending and receiving E-mail messages over the Internet. It is concluded based on the results of this study that; AEMS proved to be significantly capable of monitor the E-mail system components (E-mail server, DNS system, E-mail gateway) and detecting any failures related to those

components and provides a basis for E-mail monitoring systems techniques. AEMS consists of a set of monitoring algorithms, each of which will provide testing results and these results will be stored in the system's database used to produce user view behavior of the monitored component. AEMS system is able to alert the network administrator about the services failures in the event that the E-mail server has any problems, and works without any special requirements or conditions. AEMS have been implemented to monitor many E-mail systems in a real-working environment and the monitoring results have proven its ability to work and detect the service functionality problems.

CHAPTER ONE

INTRODUCTION

Since the arrival of E-mail system, there has been a huge need to monitor their functionality and services mainly by the losses caused by the current high dependency on these E-mail systems in communicating data between different parties. The main goal of this study is to develop an Active E-mail Monitoring System (AEMS). The proposed monitoring system is able to monitor the E-mail server protocols, queue and its services (sending and retrieving E-mail messages). The proposed monitoring system will also monitor two other major components which have direct effects on E-mail system procedures and services, namely the Domain Name System server, and the E-mail Gateway. This study will concentrate on three components (E-mail server, DNS server, E-mail Gateway) since they are considered to be the most important components in the E-mail systems. If one component is down, the process of sending or receiving an E-mail message will also be effected. AEMS consists of a set of monitoring algorithms, where each algorithm is designed for the purpose of monitoring specific component and its services within the E-mail system. Therefore, AEMS will monitor the E-mail system's functionality and services availability.

1.1 Background

E-mail systems are one of the most ubiquitous Internet-based applications today. It enables users to send and receive E-mail messages between each other. E-mail systems are used daily in almost all organizations as a communication tool

between managers, employees, customers and partners in order to improve information flow and enhance business processes requiring official documentation. E-mail system presents a fast, reliable and easy solution for such communication (Giencke, 1995; Roman, 2007).

Recently, the importance of E-mail system services has increased. The average amount of E-mail messages received per day in large organizations is relatively high. For example, in Sun Microsystems, the volume of E-mail messages exchanged between the workers per working day is about 2 million (Stebbins, 2007). In 2006, the number of E-mail messages sent over the Internet each day was 35 billion E-mail messages. In 2007, the total number was 170 billion (Nehru, 2006; Silverhart, 2007). Moreover, E-mail usage is not limited to business communication only. E-mail is also used as a communication tool between people and their friends, as a marketing tool to send advertisement messages and promotions, as an information sharing tool and as an education tool to communicate between students, their peers and their lecturers (Firoz, Taghi, & Souckova, Dec 2005; Nishida, Saitoh, Tsujino, & Tokura, 1996; Roman, 2007).

Hence, any problem occurring to an E-mail system which renders it unavailable, i.e. E-mail outage, will lead to freezing or stopping most of the daily processes dependent on the E-mail system. A good example would be universities and medium to large sized organizations (Hurst, 2004).

There are many problems which have direct affects on the E-mail system. We can divide these problems into two categories: *Planned* and *Unplanned* problems (IBM 2006). *Planned problems* can occur for many reasons, which all lead to stopping E-mail system services, such as E-mail system upgrading, E-mail management and system maintenance processes. The second type of problem are *unplanned problems*, which have a very significant impact on an E-mail system. Some of these problems can lead to more than 60 hours in outage. Various causes can lead to *unplanned problems*; some of them are due to hardware failure, connectivity loss, Storage Area Network (SAN) failure, database corruption, DNS server failure, Gateway failure, and E-mail server failure (IBM 2006; Ramesh, Venkateswarlu, & Sekharam, 2006).

This study will concentrate on the last three problems since they are considered to be the most important components in the E-mail systems. If one of those components is down, then the process of sending or receiving an E-mail message will also be down.

1.2 E-mail System

An Electronic mail system is defined as "the store-and-forward transport of electronic objects, across a heterogeneous environment, among people and application, and among applications" (Simon, 1991).

E-mail systems users use computer applications to send and receive of E-mail messages e.g. Outlook, Mozilla, and Eudora (Brain, 2008). The previous examples'

applications are called Mail User Agent (MUA). The users can send the same E-mail message to multiple users at the same time by inserting all destination E-mail addresses in the same E-mail, and sending the E-mail message to all the addresses with one click, where in this case the E-mail system is considered a broadcast system. E-mail message senders and recipients are not required to be online at the same time during the sending and retrieving process (A.Marshall, 2001).The sender can send the E-mail message at any time to the recipient's E-mail server and the recipient will retrieve the E-mail message from the E-mail server when he/she connects to the Internet, which means that the E-mail system is an *asynchronies* application. Furthermore, during the sending process there is a latency time and the E-mail message can be routed between many Simple Mail Transfer Protocol (SMTP) servers until the message reaches the destination address E-mail server. This means that the E-mail system uses a store-and-forward architecture (Giencke, 1995; Hall, 2005).

E-mail systems use the Client/Server architecture. Network clients use the MUA application to compose and send the E-mail message, which may contain various types of E-mail messages such as text, video, audio and images to the E-mail server. The E-mail server is a central component which is used to manage the E-mail messages, as in sending and receiving each E-mail message to any destination address over the Internet (Kozierok, 2005).

The E-mail system has many protocols, each of which has a specific function used to accomplish the process of sending or receiving an E-mail message. The

following section provides a brief description of the E-mail system protocols which are described in details in next chapter.

1.2.1 E-mail System Protocols

Each of the E-mail system protocols has a specific function used to accomplish the process of sending or receiving an E-mail message. The commonly used E-mail system protocols are SMTP protocol for sending an E-mail message, POP or IMAP protocol for retrieving an E-mail message and MIME method for transmitting non-text E-mail messages. Moreover, these protocols use standard ports (Halsall, 2005; Kozierok, 2005), and have standard structures used as communication tools between the E-mail clients and E-mail servers, and between the E-mail servers. The following is a brief description of these protocols:

- Simple Message Transfer Protocol (SMTP) is a transportation protocol used to transfer E-mail messages over the Internet. All E-mail servers use SMTP to send E-mails from one E-mail server to another. SMTP is also used to send E-mail messages from E-mail clients to an E-mail server. The SMTP protocol uses port 25 to accomplish the transfer process, which is one of the *well-known* ports (Halsall, 2005). This protocol resembles client/server architecture, using a set of commands which are performed during the exchange of E-mail messages between the E-mail clients and the E-mail server, or between two E-mail servers (Herardian, 2008 ; Klensin, 2001; Kozierok, 2005).

➢ Post Office Protocol (POP) is used to retrieve E-mail messages from the E-mail server. These E-mail messages have been sent to the E-mail server using the SMTP protocol. POP protocol uses port 110 or 995 to accomplish the retrieval process, (Halsall, 2005). The basic POP procedure's task is to retrieve all inbound E-mail messages from the E-mail server, store them on the client's local machine, delete them from the E-mail server and then close the connection by exchanging a list of commands between the E-mail clients and the E-mail server (Herardian, 2008 ; J. Myers & Rose, 1996; Kozierok, 2005).

➢ Internet Message Access Protocol (IMAP) is a more modern protocol which was developed in 1986. Like POP protocol, IMAP is used to retrieve E-mail messages from a remote E-mail server. The standard IMAP procedure is to leave E-mail messages on the E-mail server side instead of delivering it to the E-mail client. Thus, the users can access the E-mail server from many locations and read the incoming E-mail messages on the E-mail server. IMAP the same as POP but with more features, such as enabling the user to choose which messages to download onto a local E-mail client, as well as to create, delete and rename mailboxes, manage multiple mailboxes and download a specific portion of an E-mail message. IMAP protocol uses port 143 or 993 to accomplish the retrieval process (Crispin, 1994; Kozierok, 2005).

➢ Multipurpose Internet Mail Extensions (MIME) is a common method for transmitting non-text files via Internet E-mail system. By using this protocol, E-mail system users can send a variety of data types such as images, video and audio. MIME encodes files by using one or two methods, adding a header to a file which includes the type of data and the encoding method used and then decodes the files at the

recipient side. MIME adds the Content-Type field to the message's body format and defines the rules of non-ASCII message content, e.g. images for encoding and decoding the E-mail message (Freed & Borenstein, 1996; Patel, Henderson, & Georganas, 1994).

1.2.2 E-mail System Architecture

E-mail system architecture is divided into three major components: E-mail server, DNS server and E-mail gateway. These components are the basic infrastructure of an E-mail system, where the process of sending or retrieving an E-mail message is accomplished by using all of these components together. If one of those components is down, the E-mail system sending or receiving services will be affected.

The E-mail server is the core component of the E-mail system, where all the E-mail clients have to establish a Transmission Control Protocol (TCP) communication link with the E-mail server on a specific port for sending or receiving E-mail messages inside the local network, or to different destination addresses outside the local network over the Internet. E-mail servers uses SMTP protocol for the sending process, and use POP or IMAP protocol for the receiving process.

Domain Name System (DNS) is the standard naming system on the Internet. All the Internet services, like web browsing, or sending E-mail messages are carried out using the DNS system. DNS system is responsible for mapping from the requested domain name to Internet IP address. This process is known as the mapping

operation from a domain name to an IP address and vice versa. For the E-mail system, DNS system is used to specify the name server of the recipient's E-mail server, which is used to tell the sender's E-mail server where the outgoing E-mail messages should be forwarded to. DNS system is very important for the functioning of the Internet and the E-mail system will be effecting without DNS system resolving services (Klensin, 2003 ; Paul Albitz, 2006). The DNS system is discussed in details in chapter two.

The E-mail gateway represents the routing mechanism which solves the issue of exchanging messages between the networks via the Internet. It embodies the main interface connecting the E-mail systems with the Internet, and it is the first station on the incoming E-mail messages on the recipient's side (Halsall, 2005). The responsibilities of the E-mail gateway include receiving incoming E-mail messages and delivering them to the local recipient's E-mail server, saving a copy of all E-mail messages, starting the routing process of E-mail messages outside the local network, filtering incoming E-mail messages content, and tracking E-mail messages (Halsall, 2005; Webb, 2000). The E-mail gateway is discussed in details in chapter two.

1.2.3 General E-mail System Procedure

After the sender composes the E-mail message and issues the send command, the E-mail client queries the DNS to align the destination E-mail address to the IP address. The client then creates TCP connection with the local E-mail server. After the TCP connection is created between the E-mail client and the E-mail server, the E-mail message will be sent to the E-mail server using the client's Mail Transfer Agent

(MTA) which uses the SMTP protocol. Using the same protocol, the E-mail server will send the E-mail message to another E-mail server or directly to the recipients' E-mail server using the E-mail gateway (E-mail routing) (Webb, 2000). On the recipient side, the Mail Delivery Agent (MDA) handles the delivery process of the incoming E-mail messages to the user's inbox mail. The procedure of sending and receiving an E-mail message is explained in full details in chapter three. A detailed discussion of the sending and receiving an E-mail message using the three major components (E-mail server, DNS server, E-mail gateway) can be found in chapter two. Figure 1.1 illustrates the general E-mail system procedure.

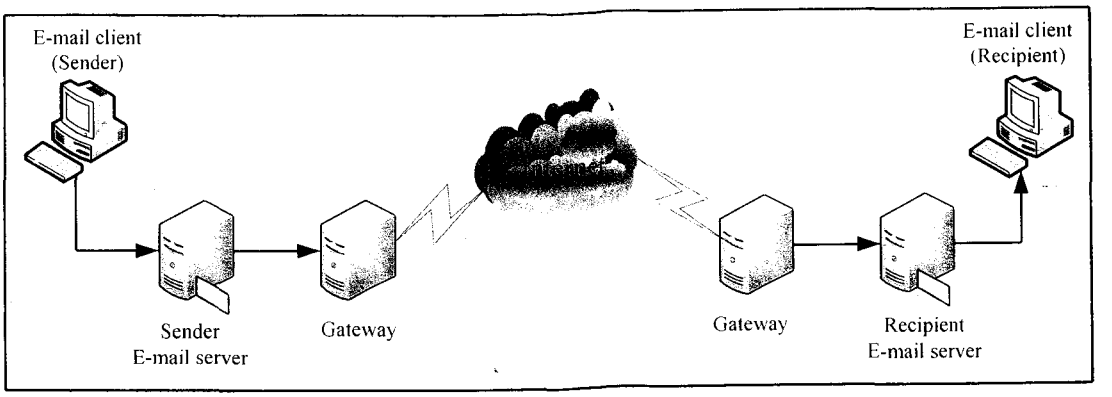

Figure 1.1: General E-mail System Procedure

1.2.4 E-mail System Monitoring Scenarios

For the E-mail system, three possible scenarios in the network architecture have been identified depending on the location of the three major E-mail system components (E-mail server, DNS server, E-mail Gateway). It is worth mentioning that the E-mail gateway is located by necessity inside the local network for the three possible scenarios. Following are the possible E-mail system scenarios:

First Scenario

The first scenario is when we have a local E-mail server in the local network responsible for sending and receiving E-mail messages to/from an Internet Services Provider (ISP) E-mail server, while the DNS server is outside the local network and uses the ISP for providing the Internet and E-mail services. Figure 1.2 illustrates the first E-mail system scenario.

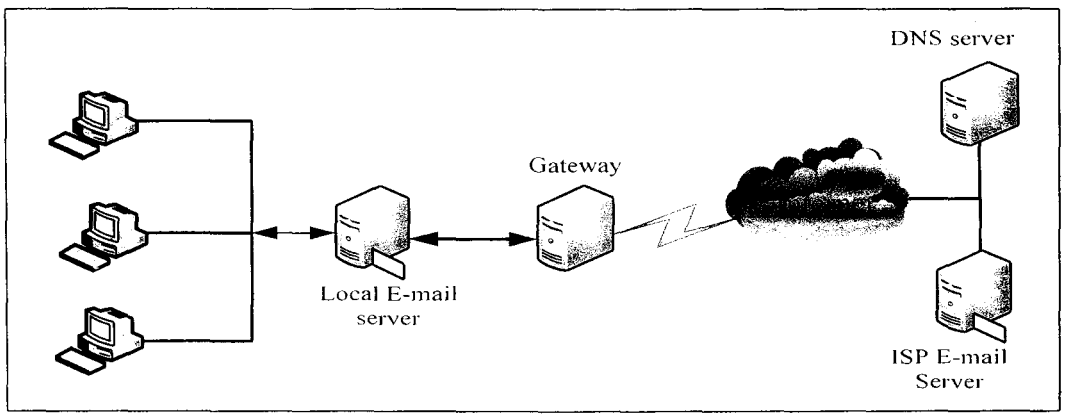

Figure 1.2: The First E-mail System Monitoring Scenario

Second scenario

The second scenario is when the E-mail server inside the local network is responsible for sending the E-mail messages from the local network to the recipient E-mail server, and receiving the E-mail messages from the local E-mail server to the E-mail client, while the DNS server is outside the local network. Figure 1.3 illustrates the second E-mail system scenario.

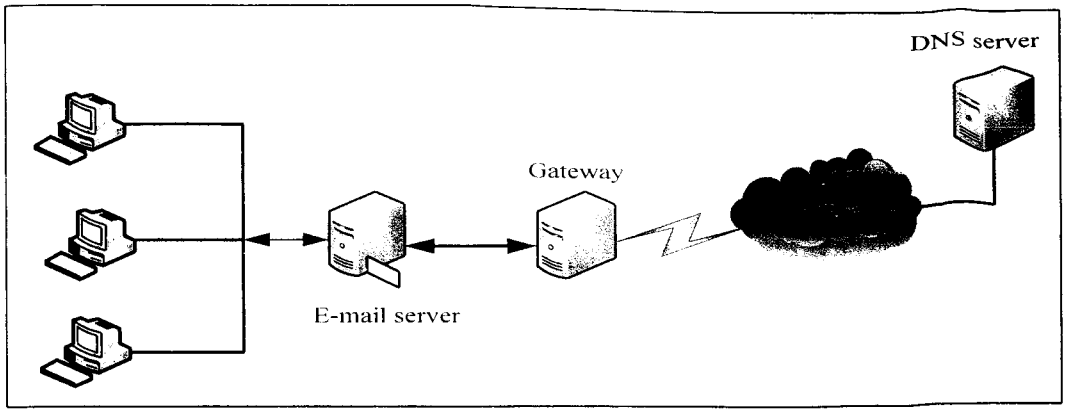

Figure 1.3: The Second E-mail System Monitoring Scenario

Third scenario

The third scenario is when all the components are inside the local network. The proposed AEMS should work under all the given monitoring scenarios. However, in this study, AEMS will be implemented to monitor and detect the failures on the last monitoring scenario only due to the experimental environment which will be discussed and used later in chapter five. Figure 1.4 illustrates the third E-mail system scenario.

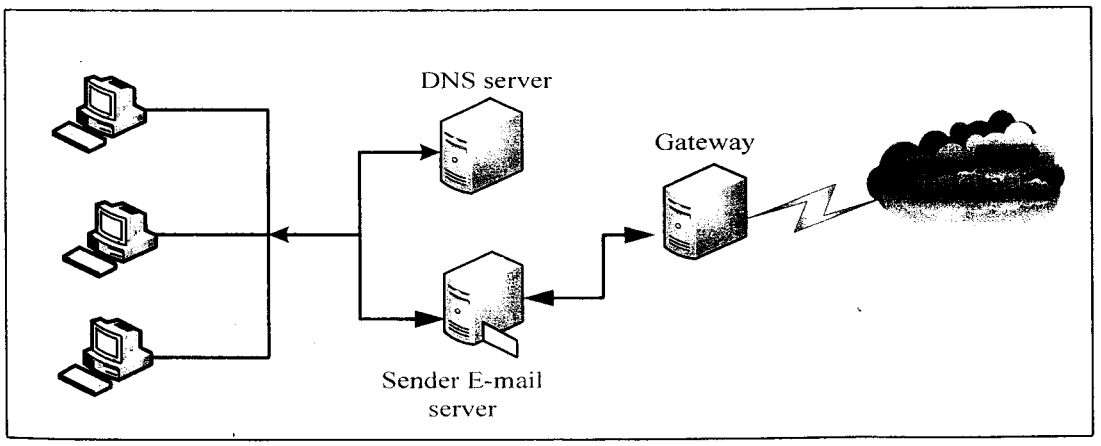

Figure 1.4: The Third E-mail System Monitoring Scenario

1.3 Active and Passive Network Monitoring

Modern network consists of a large variety of network devices. The needs of network monitoring tools to monitor, manage and maintain these devices come from the growing and expansion of the network size (Halse, 2003). Network monitoring is a system, used to monitor the network environment against failure or abnormal behaviour and to detect the breakdown of the computer network. Network monitoring systems work inside the computer network to monitor, detect the problems, determine the causes of the network problems, propose possible solutions to solve the detected network problems and perform some actions in order to solve the detected network problem. In this study, Active network monitoring will be used to monitor and detect the services failures and abnormal behaviour in the E-mail system environment (Lee et al., 2006; Mohyuddin & Dowland, 2007). Active monitoring provided more accurate information about the monitored services on the network (Bartlett, Heidemann, & Papadopoulos, 2007).

Active network monitoring is one of the network's monitoring techniques. It works by sending packets from the monitoring agent to the server or application to measure the network performance (Bartlett et al., 2007). In this technique, sending a small number of packets on the network traffic can be used to obtain the required information. On the other hand, sending a large number of packets on the network traffic sometimes leads to creating extra load on the network traffic. (Bartlett et al., 2007; Mohyuddin & Dowland, 2007).

Active monitoring is used to discover the services availability of the network components. It sends packets to a specific host (server) and monitors the response. To discover specific services, active monitoring must be designed for that service's protocol. For example, active monitoring can monitor port 25 which is the default port for the SMTP protocol, by initiating TCP connection request and monitor the E-mail servers' response on port 25 (Schryen, 2007).

Passive network monitoring is used for network fault management, for detecting network protocol problems, and for collecting very low level details about the network (Mohyuddin & Dowland, 2007). It observes the input/output of the network traffic on the server and client sides by capturing the individual packets of TCP connection on a specific port using packet sniffing software such as *TCPdump*, and studying them to determine the packet flow. The main advantage of this technique is keeping the network traffic low, because there is no need to insert additional packets to the network traffic. On the other hand, the disadvantage of this technique is the limitation of detecting the active services only and the time required for capturing the network traffic packets (Bartlett et al., 2007).

1.4 The Proposed E-mail System Monitoring Architecture

Active E-mail Monitoring System (AEMS) consists of a set of monitoring algorithms, where each algorithm is responsible for monitoring a specific function within the three E-mail system components. AEMS controls the operation of all the monitoring algorithms. It is capable of starting some of the monitoring algorithms if

required and can stop any unnecessary algorithms if the test is not required in order to produce the final AEMS.

The proposed monitoring system has the ability to monitor the three major components (E-mail server, DNS server, and E-mail gateway) in a working E-mail system environment. Each algorithm in the monitoring system will provide feedback from its testing and the results will be stored in the system's database, in order to be used by the system for providing user view behaviour of the monitored component. The final system is able to test, analyze and detect any services availability failures related to the three major E-mail system components. Figure 1.5 illustrates the AEMS architecture.

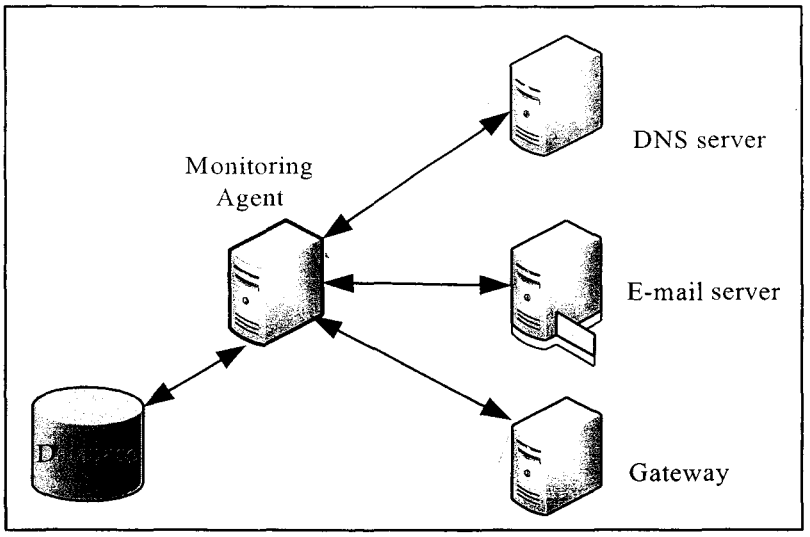

Figure 1.5: Active E-mail Monitoring System Architecture

1.5 Problem Statement

E-mail system problems can be divided into two categories: *Planned* and *Unplanned* problems (IBM 2006). Moreover, E-mail system researches have many

directions to pursue in the monitoring field. Some studies proposed techniques to monitor one or more services in the E-mail system. Duane & Finnegran (2005) divided the E-mail system monitoring into three monitoring categories, which are technical, formal and informal and proposed several alternative solutions corresponding to one or more of the address problems. Herring, Carrol, O'Grady, Coleman, & Marks (2008) and POPA (2008) have proposed that the monitoring of the network service functionality can be performed by generating a query to the network component. Škiljan & Radic (2004) provided monitoring tools working under UNIX platform.

Moreover, other studies proposed new E-mail system architectures and E-mail system protocol enhancements. Bercovici, Keidar, & Tal (2006) proposed Decentralized Electronic Mail (DEM) in order to address the centralization E-mail system shortcoming of high dependability on the central E-mail server. Tea Joon (2003) proposed a *Downmail* system for keeping and storing the outgoing E-mail messages in the sender's mailbox instead of the recipient's mailbox. Cheng & Weinong (2002) have proposed an Internet mail transfer and check system using intelligence mobile agents. Wei-Ru, Che-Hui, Chang-Ching, & Ming- Kuan (2008) have proposed a new E-mail messages retrieval architecture for the mobile users based on the concept of cache, prediction mechanism, and user behaviour in order to reduce the response time of the E-mail message retrieval process, and others studies have observed the E-mail system protocols e.g. Dekens (2006) in order to understand the relationship between the E-mail system protocols and the network traffic.

To conclude, no comprehensive E-mail monitoring system has been proposed to monitor all the E-mail system components (E-mail server, DNS server, E-mail Gateway), protocols and services, in one system, in a real-working environment.

1.6 Research Objectives

The main objective of this thesis is to design a set of monitoring algorithms based on the active monitoring, which are capable of monitoring the three major E-mail system components (E-mail server, DNS server, E-mail gateway), E-mail system functionality and services availability. This set of monitoring algorithms will Integrated into one compatible active E-mail monitoring system capable of effectively controlling the process of executing of each monitoring algorithm only when necessary in order to ensure that the E-mail system services are performing without any problems. Therefore, the objectives of this thesis are:

1. To design a set of active monitoring algorithms.
2. To integrate all the monitoing algorithms into one active monitoring system.
3. To implement the AEMS in a real-working environment.
4. To improve the AEMS ability to monitor the three major E-mail system components and detect the services availability problems.

1.7 Contribution of the Thesis

The main contribution of this thesis is Active E-mail Monitoring System (AEMS). This system is able to monitor the three major E-mail system components (E-mail server, DNS server, E-mail Gateway) in a real-working environment. AEMS

consists of a set of monitoring algorithms, each of which will provide testing results and these results will be stored in the system's database used to produce user view behavior of the monitored component. AEMS system is able to alert the network administrator about the services failures in the event that the E-mail server has any problems, and works without any special requirements or conditions.

For the E-mail system components, the monitoring algorithms have the ability to:

- Monitor the availability of the E-mail server connectivity.
- Monitor the availability of the E-mail gateway connectivity.
- Monitor the availability of the DNS server connectivity.
- Monitor the E-mail server's Queue.

For the E-mail system services, the monitoring algorithms have the ability to:

- Monitor the DNS server services and its ability for resolving domain names into IP addresses.
- Monitor Internet availability.
- Monitor the ability of the E-mail system to accept the process of creating TCP connection between the E-mail clients and the E-mail servers on a specific port number.
- Monitor E-mail system sending protocol, i.e. SMTP protocol.
- Monitor E-mail system retrieving protocols which are POP and IMAP protocols.
- Monitor E-mail server (sending and receiving E-mail messages).

AEMS have been implemented to monitor many E-mail systems in a real-working environment and the monitoring results have proven its ability to work and detect the service functionality problems (see chapter five).

1.8 Thesis Outlines

This thesis is organized into six chapters. This chapter introduces the E-mail system components and our research objective and contribution. Chapter two will review literature related work to the E-mail monitoring system and E-mail system enhancement.

Chapter three covers two parts. The first part provides a full description about E-mail system sending and receiving procedure. The second part covers the methodology and the design of the proposed monitoring system and its monitoring algorithms.

Chapter four covers of the implementation details of the proposed monitoring system. Chapter five describes the experimentation direction and the testing scenarios and results in a real-working E-mail system environment. Chapter six provides the summary of this thesis and suggestion for future work.

CHAPTER TWO

E-MAIL SYSTEM MONITORING RELATED WORK

This chapter will explore the previous studies of E-mail systems. We begin with an overview of the history of E-mail systems and the evolving process. We will also discuss DNS system, E-mail system protocols (TCP, SMTP, POP and IMAP), the studies on the E-mail system monitoring and E-mail system enhancement, as well as a summarization of the previous work. Previous work shows that E-mail system researches have embarked in many directions, with some proposing new E-mail system architecture, E-mail system protocol enhancements and observing E-mail system protocols. The main challenge encountered in this study is the lack of related work focused on monitoring E-mail systems and their components. The related works are divided into a set of categories based on the components of the E-mail system. We will begin with a narration of the history of E-mail systems, followed by a review of the previous research on E-mail systems focusing on the diversity of monitoring technique. Thereafter we discuss the E-mail system enhancements made in this field. We conclude the chapter with a summary of the overall work done.

2.1 E-mail System History

The rapid growth of the Internet and the needs for communication tools led to the invention and development of E-mail systems. Nowadays, E-mail system are the most popular computer-based application on the Internet. E-mail system is one of the basic network services which was developed during the use of Advanced Research Project Agency Network (ARPANET) network between 1970s and 1980s, where the

E-mail system was developed as an application for the ARPANET network (Hardy, 1996).

E-mail system development started in 1960s and the driving the reason was to allow for the exchange of text and messages between the users of time-sharing computers (Croker, 2008; Hardy, 1996; Partridge, 2008). In 1971, an ARPANET E-mail application was developed in order to provide the ability to copy files over the network and to send them in the form of an E-mail message. Moreover, the format of the E-mail message was developed by using the (@) sign to combine the user and the host name (Hardy, 1996; Partridge, 2008). In 1972, the File Transfer Protocol (FTP) program was used to improve the network transport capabilities for E-mail transmission (Croker, 2008). In 1973, a program that has the ability to work with E-mail headers and to sort or list subject and date was developed in order to allow the user to retrieve the E-mail messages in his/her inbox and to reads, saves or deletes them (Hardy, 1996; Postel, 1982). In 1975, a project was initiated to develop the Message text (MSG) program for UNIX operating system. Unfortunately, it was very slow to obtain more benefits from MS. The result from that division was called Mail Handles (MH) application, which continued upgrading until 1982 where it became the standard E-mail application for the UNIX environment (Croker, 2008; Partridge, 2008; RAND, 2009). In 1978, Multi-Purpose Memo Distribution Facility (MMDF) was developed, which provided relay E-mail over dial-up to the sites that could not connect directly to the ARPANET (Croker, 2008). In 1980 Mail Transfer Protocol MTP was published in RFC 772 and it was revised later to SMTP protocol (Kozierok, 2005). In 1981, the Simple Mail Transport Protocol (SMTP) was developed. SMTP enabled a single message to be sent to a domain with more than

one recipient's address, after which the local server would locally copy the message to each recipient (Partridge, 2008). In 1988, the first E-mail client program to provide graphical interface was written and it was called Eudora. However, Eudora was quickly supplanted with the emergence of the Netscape and Internet Explorer (Hardy, 1996; NSF, 1993). In 1993, a large scale adoption of Internet E-mail as a global standard began (Croker, 2008), and since that time several reviews were introduced e.g. RFC 2034 and RFC 5321.

2.2 E-mail System Components

This section will discuss the main features and procedure for the DNS, the E-mail gateway and the E-mail system protocols which have direct effect on the E-mail system procedures, its services and functions.

2.2.1 Domain Name System (DNS)

There are millions of hosts connected to the Internet every day. Each host must have a unique name. When any user on the Internet attempts to access web page, or sending an E-mail message, the client uses the unique name to accomplish the required operation (Gouda, 2005). To access web page or complete the process of sending an E-mail message, the users are using domain names rather than IP addresses which are easier to remember for browsing and E-mailing. On the other hand, Internet hosts communicate with each other using IP address, where for each unique name there is a unique IP address. To accomplish browsing or E-mailing process, unique names must be translated into a unique IP addresses first, and this is

known as name-to-address is mapping. This process can be done using Domain Name Servers System (Brain, 2008; Gouda, 2005).

The structure of DNS name space is a hierarchical structure, where the node on the top of the tree is called root domain. Root domain node has many nodes in the top-level domain names such as COM, NET, ORG, INFO and EDU. Each domain has one or more nodes associated with it and the last node in the lowest level is the host which is attached to the Internet. Each node which or domain name in the tree has a string of labels which is used to identify the node to its parent (Gouda, 2005; Halsall, 2005; Paul Albitz, 2006). For example domain *www.nav6.org* consists of root domain which is the "." Character, top-level domain which is the "org.", second-level domain which is "nav6.org.", and the third-level domain "www.nav6.org." . The dot character (".") is very important and it is used to indicate to the domain name as Fully Qualified Domain Name (FQDN) (Barr, 1996; Gouda, 2005; Paul Albitz, 2006) .

Domain name space is divided into a number of zones (Halsall, 2005; Paul Albitz, 2006). Each zone has name servers which are responsible for this domain and each is controlled by the higher-level domain. Each zone contains all information about this domain. This information is stored as resource records consisting of a string of labels (Halsall, 2005; Paul Albitz, 2006). One filed in the string labels is named *type*, which refer to the type of the record. Moreover; there are many types of the records, the record can be "A-record" which contains the IP address which is assigned to this domain name, "NS record" which contains a list of the name servers which are authoritative for this domain, (Star of Authority) "SOA record" which

contains information about handling the zone, "MX record" which contains the mail server names which is responsible about this domain and Canonical name "CNAME record" which contains aliases name for this domain (Barr, 1996; Halsall, 2005; Paul Albitz, 2006) . Figure 2.1 illustrates the DNS system architecture.

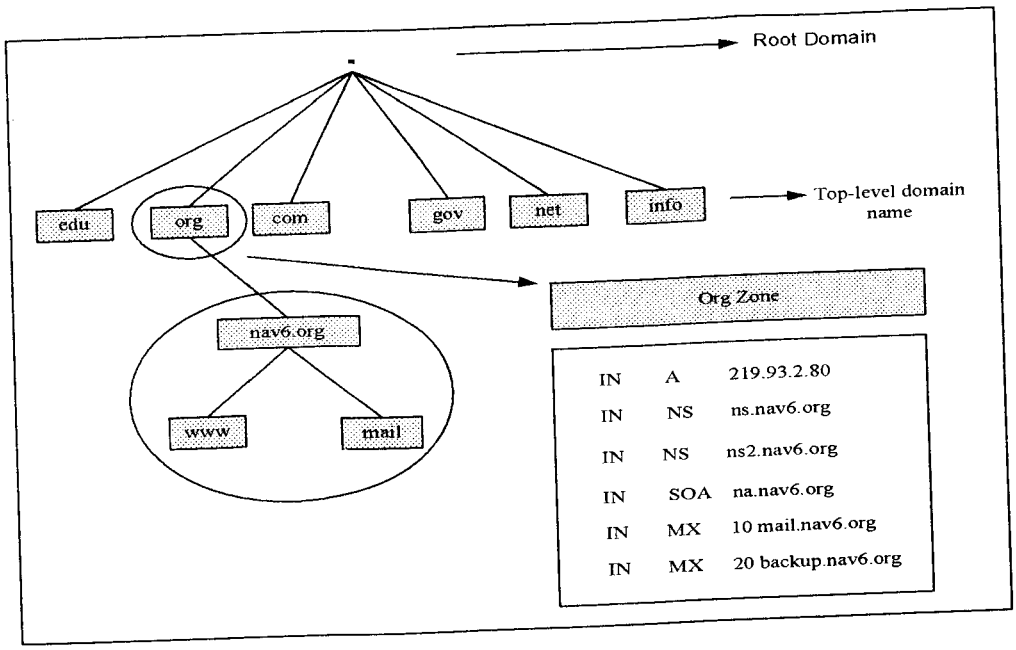

Figure 2.1: DNS System Architecture

Name servers have two response behaviours to resolve a domain query into IP address. Name servers are *authoritative* when the name servers respond to the domain query by using the local domain data. Name servers are *non-authoritative* when the name servers query another authoritative name server in order to resolve the requested domain to IP address (Barr, 1996; Paul Albitz, 2006). Name servers answers can be categorized into the following:

- Answer the requested domain name and return the IP address.
- Connect with other name server in order to retrieve the answer and [illegible] address.
- Return another IP address which is pointer to another name server [illegible] ability to return the IP address answer.
- Return error message which indicates that the requested domain name is [illegible] invalid name.

When the name server receives a new domain name query, it first checks the local recourse records to find an answer, if name server has an answer; it sends it back to the resolver. Otherwise; name server checks the local cache memory to find an answer. If the cache memory has an answer, then name server uses the cached information to send back the answer. Otherwise; the name server starts a *"recursive query"* until it finds an answer and caches the new answer (Cohen & Kaplan, 2001; Paul Albitz, 2006). Figure 2.2 illustrates the recursive query and caching procedure.

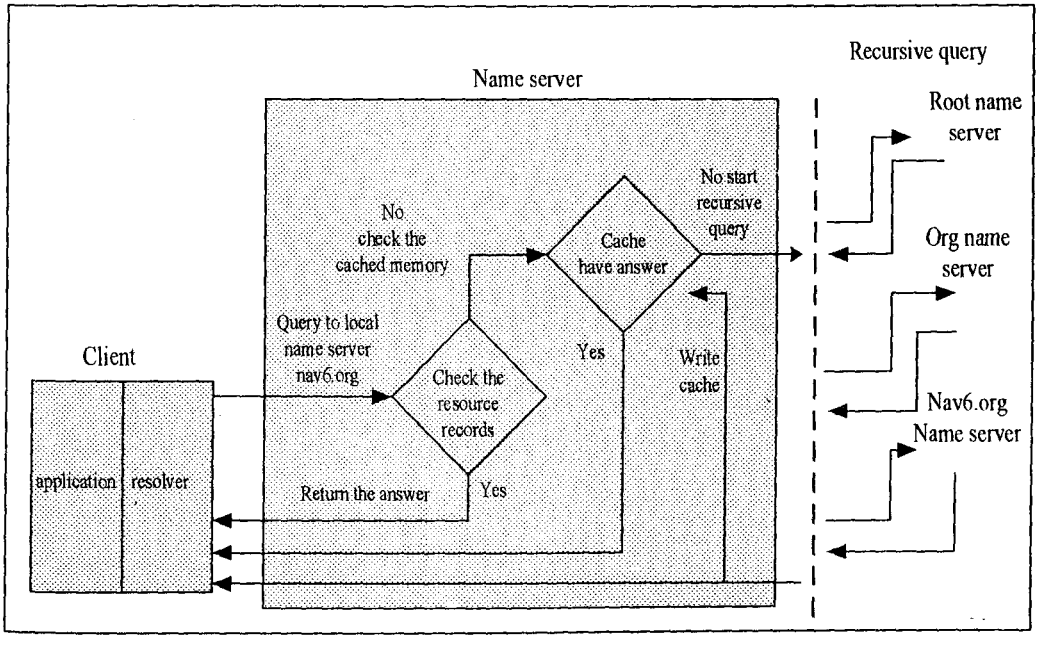

Figure 2.2: DNS Name Server Caching and Recursive Query