NETWORK ALARM REPORTING SYSTEM

MUHAMMAD AL-HAFIDZI BIN MOHAMMAD SALLEH

A report submitted in partial fulfillment
of the requirements for the award
of degree of

Bachelor of Computer Science (Computer System & Networking)

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

NOVEMBER, 2005

ABSTRACT

Traditionally, network management activities, such as fault management have been performed with direct human involvement. However, these activities are becoming more demanding and complex due to increasing size of networks in information technology today. For that reason, it is becoming necessary to automate network management activities. In KUKTEM network environment, the notification of a network failure in KUKTEM has not reached the demanding of higher technology yet. Network administrators acknowledge the network failure within the working hour only. The problem is they do not acknowledge network failure which occurred out of working hour. So, they are wasting time of delaying fixing network problems. Advance concept in Network Alarm Reporting System (NARS) can play an important role in the network problem solving that is employed in fault management. The successful phases indicated in this system have been successfully applied to the network management system. NARS provide a good solution to overcome the network alarm in KUKTEM. The continuous monitoring process from NARS will increase the quality of network management skills. The verification of network failure and notification report is an efficient way to manage network successfully. In the notification process, NARS provide reliable and fast services by applying Short Message Services as a medium of delivering report.

ABSTRAK

Kebiasaannya, di dalam pengurusan rangkaian seperti pengurusan kesilapan dalam rangkaian adalah melibatkan manusia. Walau bagaimanapun, pengurusan rangkaian seperti ini adalah memerlukan keterampilan yang tinggi mengikut kepelbagaian rangkaian dan saiz rangkaian yang semakin besar. Oleh sebab itu, pengurusan rangkaian secara automatik adalah amat diperlukan. Lebih-lebih lagi, teknologi dalam pemberitahuan tentang kesilapan dalam rangkaian adalah di tahap yang sangat rendah di dalam persekitana rangkaian KUKTEM. Pengurus rangkaian mengetahui tentang masalah rangkaian di dalam KUKTEM adalah di dalam waktu kerja sahaja. Mereka tidak dimaklumkan tentang masalah rangkaian di luar waktu bekerja sahaja. Mereka tidak dimaklumkan tentang masalah rangkaian di luar waktu bekerja. Oleh itu, mereka telah merugikan masa dalam menyelesaikan masalah tersebut. Beberapa konsep dalam system ini memainkan peranan penting dalam teknik penyelesaian masalah rangkaian. Lebih-lebih lagi, fasa-fasa yang telah diaplikasikan dalam sistem ini telah berjaya mengatasi masalah dalam pengurusan rangkaian. Untuk mengatasi masalah rangkaian yang berlaku dalam KUKTEM, system ini adalah penyelesaian yang paling bagus. Sistem ini memberi servis yang pantas dan mantap bermula daripada mengesan masalah rangkaian sehingga pemberitahuan masalah kepada pengurus rangkaian. Pengawasan rangkaian secara berterusan daripada system ini dapat meningkatkan kualiti dalam kemahiran menguruskan rangkaian. Notis pemberitahuan tentang masalah rangkaian yang efektif dalam system ini juga adalah satu cara yang berjaya dalam menguruskan rangkaian. System ini akan menjana satu mesej yang akan dihantar melalui pesanan teks ringkas menerusi telefon bimbit apabila berlaku masalah rangkaian.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURES

LIST OF ABBREVIATIONS

GSM	-	Global System for Mobile Communication
SMS	-	Short Message Services
NMS	-	Network Management System
SNMP	-	Simple Network Management Protocol
CMIP	-	Common Management Information Protocol
ISO	-	International Standard Organization
TCP/IP	-	Transfer Control Protocol/ Internet Protocol
SDLC	-	Software Development Life Cycle
ICMP	-	Internet Control Message Protocol
KUKTEM	-	Kolej Universiti Kejuruteraan & Teknologi Malaysia

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Security is needed to keep network environment in safety condition. One of security medium is delivering alarm. In networking technology, network alarm is required to provide security.

Alarm can be described to a device which can make an acknowledgement or alert when something goes wrong or fail to function. For this system, alarm is not a device with noisy sound or buzzing. It is just some alert sent by a package of message for notification in network environment which called network alarm. Network alarm is the alert that made by networking device or system to notify an administrator after their network goes wrong.

1.2 Problem Statement

There are so many technologies in alarming system such as car alarm, home fire alarm and other computer based alarm. An intrusion or network failure is usually easy to detect if it happened during working hour. But, those failures cannot be noticed if it happens out of working hour. There would be a long period while network down time approximately about seven to eight hours according to the observation.

Any task using network could not be done within those times before fixing. In KUKTEM, student cannot send memo and using internet for searching some information while those network failures occurred.

To prevent these problems we need Network Alarm Reporting System (NARS). This system is to mention network administrator who is out of working hour which the notification delivered via Short Message Service (SMS). The alarm reporting will be delivered at any time and any place through mobility device such as cellular phone.

1.3 Objectives

The are objectives of this system are:-

i. To give an acknowledgement to network administrator after device failure.
ii. To notify network administrator about information on device failure before network fixing.
iii. To make enhancement in current network alarm in KUKTEM by providing SMS notification.

1.4 Scope

NARS will be implemented in KUKTEM network environment. NARS will detect the condition of a host within a period of time. If the network line goes down, NARS will detect a device failure then compile a message of report and send it to network administrator. The medium for message report is using Short Message Service (SMS) which delivered by GSM phone.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Network Alarm Reporting System is the part of network management system. Network management can be described by process of controlling a complex data network to maximize its efficiency and productivity. Considering of impact of security in network management system is important because core-business revenue depends increasingly on network whose availability and performance are critical for survival. The university network is backbone of mission-critical application and the vehicle that student use to access information and services.

When network fails, students and lecturers cannot communicate; cannot access need information and applications including memo and email services. Thus, productivity will suffers and revenue stop flowing. By minimizing downtime and network performance degradation, network management systems allow business to operate more efficiently, cut costs and prevent revenue loss. The person who takes this responsibility to reduce network downtime is network administrator.

As an administrator, he needs to monitor traffic on his network. With network monitor, he can gather information about the network traffic that flows to and from network adapter of the computer which act as a network server. The advantage of using

NARS is the notification phase which implements a SMS report which is more effective instead of using sound alert or email for delivering report to network administrator.

2.2 Network Management

Network management means different things to different people. In some cases, it involves a solitary network consultant monitoring network activity with an outdated protocol analyzer. In other cases, network management involves a distributed database, auto polling of network devices, and high-end workstations generating real-time graphical views of network topology changes and traffic. In general, network management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks (Cisco Systems. Inc, 2002).

2.2.1 Network Management Architecture

Most network management architectures use the same basic structure and set of relationships. End stations such as computer systems and other network devices, run software that enables them to send alerts when they recognize problems. Upon receiving these alerts, management entities are programmed to react by executing one, several, or a group of actions, including operator notification, event logging, system shutdown, and automatic attempts at system repair (Cisco Systems. Inc, 2002).

Management entities also can poll end stations to check the values of certain variables. Polling can be automatic or user-initiated, but agents in the managed devices respond to all polls. Agents are software modules that first compile information about the managed devices in which they reside, then store this information in a management database, and finally provide it either proactively or reactively to management entities

within network management systems (NMSs) via a network management protocol. Well-known network management protocols include the Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP). Management proxies are entities that provide management information on behalf of other entities (Cisco Systems. Inc, 2002).

The ISO has contributed a great deal to network standardization. Its network management model is the primary means for understanding the major functions of network management system (Cisco Systems. Inc, 2002). This model consists of five conceptual areas:-

i. Performance management
ii. Configuration management
iii. Accounting management
iv. Fault management
v. Security management

2.2.1.1 Performance Management

The goal of performance management is to measure and make available various aspects of network performance so that internetwork performance can be maintained at an acceptable level. Examples of performance variables that might be provided include network throughput, user response times, and line utilization.

Performance management involves three main steps. First, performance data is gathered on variables of interest to network administrators. Second, the data is analyzed to determine normal or baseline levels. Finally, appropriate performance thresholds are determined for each important variable so that exceeding these thresholds indicates a network problem worthy of attention (Cisco Systems. Inc,2002).

Management entities continually monitor performance variables. When a performance threshold is exceeded, an alert is generated and sent to the network management system.

Each of the steps just described is part of the process to set up a reactive system. When performance becomes unacceptable because of an exceeded user-defined threshold, the system reacts by sending a message. Performance management also permits proactive methods: For example, network simulation can be used to project how network growth will affect performance metrics. Such simulation can alert administrators to impending problems so that counteractive measures can be taken (Cisco Systems. Inc, 2002).

2.2.1.2 Configuration Management

The goal of configuration management is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

Each network device has a variety of version information associated with it. An engineering workstation, for example, may be configured as follows:

i. Operating system, Version 3.2
ii. Ethernet interface, Version 5.4
iii. TCP/IP software, Version 2.0
iv. NetWare software, Version 4.1
v. NFS software, Version 5.1
vi. Serial communications controller, Version 1.1
vii. X.25 software, Version 1.0
viii. SNMP software, Version 3.1

Configuration management subsystems store this information in a database for easy access. When a problem occurs, this database can be searched for clues that may help solve the problem (Cisco Systems. Inc, 2002).

2.2.1.3 Accounting Management

The goal of accounting management is to measure network utilization parameters so that individual or group uses on the network can be regulated appropriately. Such regulation minimizes network problems because network resources can be apportioned based on resource capacities and maximizes the fairness of network access across all users (Cisco Systems. Inc, 2002).

As with performance management, the first step toward appropriate accounting management is to measure utilization of all important network resources. Analysis of the results provides insight into current usage patterns, and usage quotas can be set at this point. Some correction, of course, will be required to reach optimal access practices. From this point, ongoing measurement of resource use can yield billing information as well as information used to assess continued fair and optimal resource utilization (Cisco Systems. Inc, 2002).

2.2.1.4 Fault Management

The goal of fault management is to detect, log, notify users of, and automatically fix network problems to keep the network running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements (Cisco Systems. Inc, 2002).

Fault management involves first determining symptoms and isolating the problem. Then the problem is fixed and the solution is tested on all-important subsystems. Finally, the detection and resolution of the problem is recorded (Cisco Systems. Inc, 2002).

2.2.1.5 Security Management

The goal of security management is to control access to network resources according to local guidelines so that the network cannot be sabotaged either intentionally or unintentionally and sensitive information cannot be accessed by those without appropriate authorization. A security management subsystem, for example, can monitor users logging on to a network resource and can refuse access to those who enter inappropriate access codes (Cisco Systems. Inc, 2002).

Security management subsystems work by partitioning network resources into authorized and unauthorized areas. For some users, access to any network resource is inappropriate, mostly because such users are usually company outsiders. For other internal network users, access to information originating from a particular department is inappropriate. Access to Human Resource files, for example, is inappropriate for most users outside the Human Resources department (Cisco Systems. Inc, 2002).

Security management subsystems perform several functions. They identify sensitive network resources including systems, files, and other entities and determine mappings between sensitive network resources and user sets. They also monitor access points to sensitive network resources and log inappropriate access to sensitive network resources (Cisco Systems. Inc, 2002).

According to the five conceptual areas that have been showed, only one concept will be implemented in NARS which is fault management. Fault management consist fault analysis which must be deployed in order to find the faulty of a network. One of the ways to find the network faulty is through network monitoring.

2.3 Network Monitoring

Network monitoring is a way of networking field to monitor an ip-based device or system that is on the network. Network monitoring can be an effective way to monitor and analyze the design of LAN for administrator, security professional or network programmers. Actually network monitor is for everyone who wants a full picture of the traffic flowing through a PC or LAN segment (Network-Monitoring.com; 2002).

Network monitoring can captures every packet on the wire or wireless to display important information such as a list of packets and network connections, vital statistics, protocol distribution charts, and so on.

Network monitoring allows user to capture network traffic on any computer where remote host is running, regardless of the computer's physical location. This powerful and unique technology broadens the monitoring range. Users are no longer limited by LAN segment or personal computer (Network-Monitoring.com; 2002).

Network monitoring also help user maintain efficient network data transmission, test firewalls and intrusion detection systems, or identify problems with network-based applications. Besides that, there is an important economic reason behind using a network analyzer which it costs a fraction of the price of information, time, software, and hardware that may potentially be lost or wasted by not using a network analyzer (Network-Monitoring.com; 2002).

2.3.1 Benefit of Network Monitoring

The benefits are limitless - monitoring in network can only be beneficial to network administrator and the company. See some common reasons that explain how priceless monitoring can be.

i. Recover lost communication

With the increasing use of email, chat, and instant messaging among the workplace as a form of communication the more traditional forms of telephone and written letters are falling (Network-Monitoring.com; 2002).

ii. Eliminate leaking of confidential information

One of, if not the most important, assets in the company is the information withhold. This being trade secrets, source code and programming, records, customer information and contacts, strategies, product development, and much more. Internet activities now have records of the activities that have been done through network by monitoring it (Network-Monitoring.com; 2002).

2.4 Current Network Monitoring System

This is a current system for network monitoring system that have been tested. Free Visual Ping version 3.4 is the latest version from ITLight Software company.

2.4.1 Visual Ping

Free Visual Ping is a network diagnostic tool for Windows platforms. Using this tool you can monitor TCP/IP targets, by sending packages to those targets and viewing the received packages result over a detailed list and a graph. Free Visual Ping is an easy to use replacement for the standard ping utility. The ping process verifies connectivity to a host on local area network or on the Internet. Ping sends an ICMP *echo request* as a data packet to a remote device and displays the results for each *echo reply*. This exchange is called *pinging* (ITLight Software , 2005).

Ping sends one packet per a period of time of user choice and prints and draw one line of output for every response received. When ping terminates, it displays a brief summary of round-trip times and packet loss statistics. Round trip times indicate the time (in milliseconds) it takes for the packet to get to the remote host and a response to arrive back. This time varies depending on network load (ITLight Software , 2005). Refer Figure 2.1 for details.

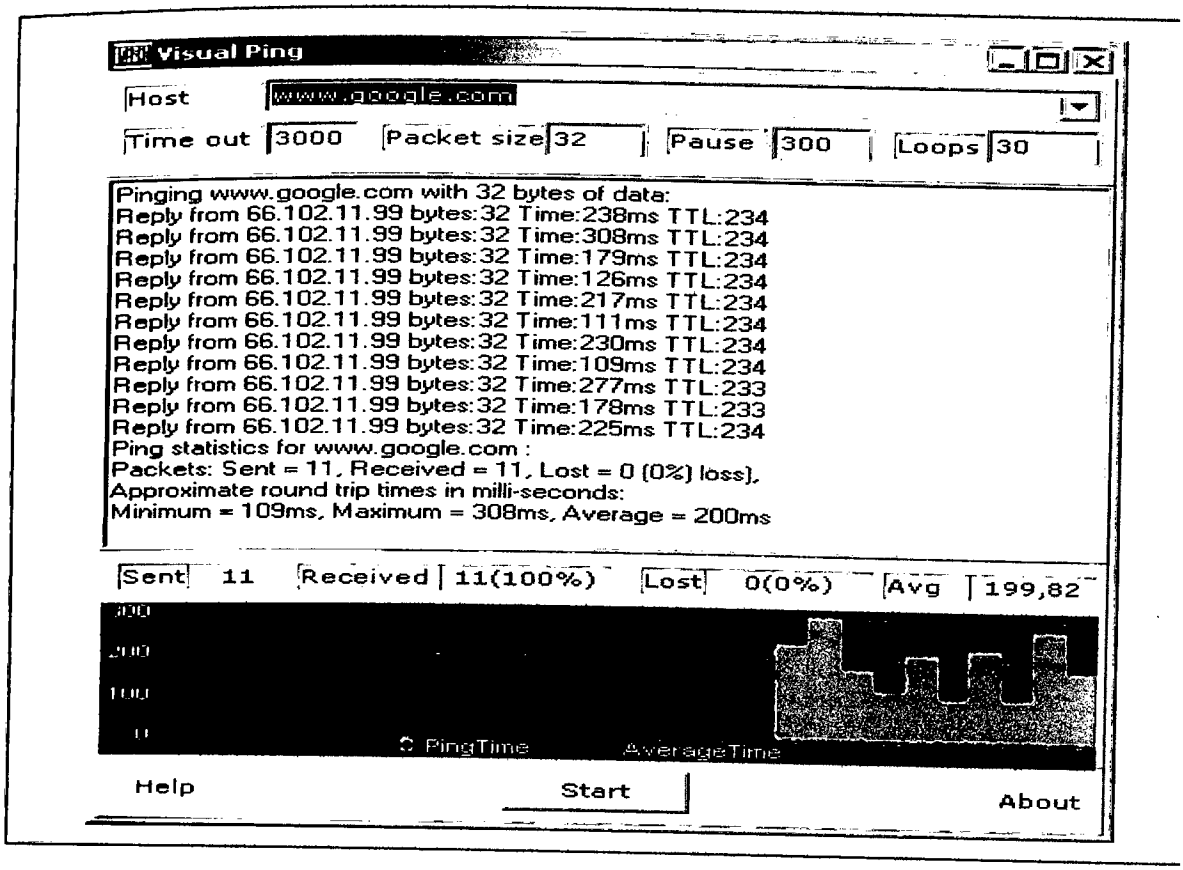

Figure 2.1 Interface of Visual Ping

2.5 Major Component in NARS

A framework for automating fault management is presented in NARS. The management function is to correlate the real problem whether the device is having problem or not after monitoring phase. NARS implement ICMP for its monitoring protocol.

In order to perform the fault management process, 2 network element needs to be applied in this system which includes:

i. Internet Control Message Protocol (ICMP)
ii. Short Message Service (SMS)