International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN : 2278-800X, www.ijerd.com
Volume 5, Issue 7 (January 2013), PP. 89-96

Remote Administration of Network Servers Using Short Message Service

A. Raghavendra Rao[1], B. Kishore Kumar[2]
[1,2]Aditya Institute of Technology and Management

Abstract:- There is always a great concern for network administrators, how to deal with network failure in reasonable time span. Network failure can happen any time of the day and administrator may not be informed in time and even then would not be able to enforce the remedy effectively. This scenario will arise when physical access to the network devices is not possible; i.e. the administrator is away from network locations. In this paper a new approach has been adopted in such a way that, the information on network status is gathered by an application, using SNMP protocol and is sent to network administrator by SMS. This approach also will allow network administrator to apply all necessary commands, using SMS. The short messages are then converted to be used by SNMP protocol to rectify faults, causing network failure.

Keywords:- component; AT Command, Community, GSM Modem, SMS, SNMP

I. INTRODUCTION

Data communication and computer networking facilities are expanding rapidly. Proportional to this expansion, problems relating to network control and administration have also been increased. Physical presence of network administrator or remote access via Internet are identified as common solution to this problem. In these approaches the network administrator will investigate all aspects of network operation and under his access privilege intervene and apply necessary commands. SNMP [1, 2 and 3] and CMIP [4] are two popular network management protocols, however SNMP is a simpler and more favorite than the CMIP. SNMP is used to acquire information on network operation status, generation of reports and applying corrective commands to the network devices under administration.

In this paper a new approach to network administrator has been adopted which uses the SNMP protocol, based on short message services (SMS) [5]. An application is installed on a system which has access to the network under administration. Upon the administrator request, all necessary information will be gathered by this application, using SNMP protocol and then is sent to the administrator via short message service, SMS. In turn the administrator is able to issue commands with certain format applicable to the SMS, to the same application. At this stage the application with the collaboration of SNMP, the issued command will be applied to the target device.

The proposed system has been implemented and evaluated in both experimental and real network at Yazd University. Under both circumstances the results show that there would be a drastic reduction of network downtime as well as capability to produce varieties of reports from the network which is being administered. This paper deals with the details of the proposed system in several sections. Section two introduces the SNMP protocol and section three will explain the way short messages are sent and received. Section four is allocated to describe the overall structure of proposed system and in section five the security aspect of this system has been explored. In section six our system is evaluated and following section will discuss some of the related research work. The final section will deal with the outcome of this research work and the conclusion.

II. INTRODUCING SNMP PROTOCOL

Simple Network Management Protocol is designed with the objective to facilitating the management of network devices, exchange of management related information and communication with different devices within the network. In essence this protocol allows the network administrators to measure the network performance, to trace and locate the network malfunctions and subsequently react to such circumstances. Some relevant part of SNMP protocol for implementation of this work is discussed briefly, however more information can be found at [1, 2 and 3].

A. Basic SNMP Messages

A SNMP message can be created either by the network administrator or by a device within the **same** network. In SNMP protocol TRAP, GET and SET messages are considered as basic messages. The TRAP

message [6] is created by a device within the network for warning or when there is a failure, such as lack **of** paper for printer or a router link failure. The GET message is applied when the network administrator intends to acquire some information from a device. For example a WAN link status may be monitored every five minutes. In this case not only the received information can present the link status, it can also relay this information to the report generating system. The SET message is used by network administrator to modify an intended parameter of a device. An example of SET message is to change a static route on the router within the network.

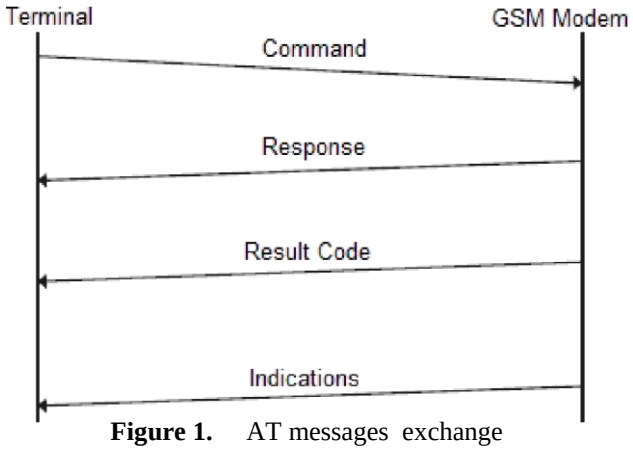

Figure 1. AT messages exchange

B. SNMP Management Information Base (MIB)

The MIB are a set of comprehensive variables that are used in a uniform and standard fashion among all of the devices within the network and the network management system [7]. The MIB is expandable in such a way that the hardware or software vendors can introduce a new set of variable to the existing table. However the new variables must initially be introduced to the both network management system and devices of the network.

C. Community within the SNMP

The most fundamental aspect of security for the SNMP is communities [8]. Communities act as passwords for access to the network devices. Commonly one community is set for only read access to a network device. However there are communities that allow read and write access to a device. The default values for read only communities are set as "public" and for read and write communities are set as "private". These communities allow the network management system modify the MIB variables of the network.

III. SENDING AND RECEIVING SHORT MESSAGES FROM A WORKSTATION

A GSM modem [9] with high baud rate is required to send and receive short messages from a work station. The work station must utilize the standard AT (attention) commands [10], to be able to use GSM modem. It is evident that nearly all mobile phones with USB connection port will support the AT commands and thus are able to function as a GSM modem. Practical implementation of this work is necessitated to use GSM modem, to be able to send and receive short messages with high speed at any given time. However there is no doubt that within a limited network management system, the GSM modem can be replaced with mobile phone with USB port.

When a GSM modem or a mobile phone is connected to a work station, initially its driver must be installed. The driver act as a middleware to facilitate compatibility of applied commands to the specific hardware under use. For instance if a mobile phone to be used for implementation of this work, it
Would have been required to download its middleware from the vendor's support site and then to install on work station. In this case it would have created a virtual GSM modem on one of the work station's port, where communication on this port could be programmed.

In order to simplify the AT commands and avoid the detail of coding messages, it is recommended to use the libraries of short messages for send and receive. The programmer can use these libraries to open ports, recognizing the communicating devices connected to the work station, send and receive short messages, classes, methods and high level events.

A. AT Commands

AT commands are a set of commands to control the modem. The connection initiates from a terminal, therefore it requires each service to be requested by the terminal. This request is an AT command. Each command has a result code indicating the status of that command and a reply containing the modem data (figure 1). The AT commands usually starts with AT prefix and are different from standard modem supporting

commands. The AT commands are commonly used for:

- Dialogue services: dialing and termination
- Short message services: send and receive SMS
- Network query services: network's signal quality

The expected performance of GSM, using the relevant commands and capability of providing send/receive services of short messages are the objective of this paper. Table 1 depicts the list of commands, used for sending and receiving short messages.

B. Application of AT Commands

To apply the AT commands to the modem, an application such as Hyper Terminal could be used, but we implemented our application to meet the required features. This application simply forwards a command to the modem and returns back the modem's reply.

TABLE I. AT COMMANDS TO TRANSMIT SHORT MESSAGES

Row	Command	Description
1	Send Message	+CMGS
2	Send Message From Memory	+CMSS
3	Write to Memory	+CMGW
4	Delete Message	+CMGD
5	Send Command	+CMGC
6	Send More Messages	+CMMS
7	Indicating New Message	+CMMI
8	List Message	+CMGL
9	Read Message	+CMGR
10	Acknowledge New Message	+CMMA

The following is an example of sending short message via Hyper Terminal program.

```
AT
OK
AT+CMGF=1
OK
AT+CMGW="+989354965764"
> A simple SMS text messaging.
+CMGW: 1

OK
AT+CMSS=1
+CMSS: 20

OK
```

The following is an example of receiving a short message via Hyper Terminal

```
AT
OK
AT+CMGF=1
OK
AT+CMGL="ALL"
+CMGL: 1,"REC READ","+989354965764",,
"06/11/11,00:30:29+32"
Hello, welcome to our SMS tutorial. +CMGL:
2,"REC                READ","+85291234567",
,"06/11/11,00:32:20+32"
A simple SMS text messaging.

OK
```

IV. PROPOSED STRUCTURE OF NEW SYSTEM

In our proposed system the network devices shall transmit warnings and messages to the network administrator, using SNMP protocol. The network administrator can receive these messages via Short message service and if necessary, he can send and apply a command to a specific device on the network, using SMS. In Addition the network administrator is able to log the status of any individual device by SMS. The architectural aspect of this system is shown in figure 2.

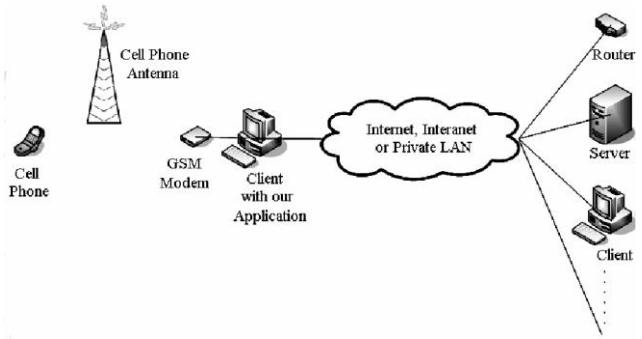

Figure 2. The architecture of proposed system

The core functionality of this system is an application program, installed on the work station equipped with GSM modem and has access to the target network. The application program communicates with network devices via private LAN or Internet or intranet, in conjunction with SNMP protocol. The main tasks of this application program are:

1) To receive a message from a network device with the use of SNMP protocol,
2) Converting it to the short message protocol,
3) Sending short message to the network administrator and also
4) Receiving short message from network administrator,
5) Conversion of a command to an appropriate MIB and SNMP protocol,
6) To apply the network administrator's command to the network device.

The middleware application program expects to receive a short message from network administrator and then authenticate the access right of the message source. The authentication process uses the information embedded within the short message (i.e. the caller ID or the community name in the text message). When the message is received and authenticated, shall be applied to the specified network device, using SNMP protocol and the result is sent back to the message source. Further more the middleware application program will eardrop for any warning from network devices and the collected information shall be conveyed to the network administrator in the form of short messages. In addition the network administrator can monitor the network status at any time by applying the SNMP commands. AS an example a command can be issued to monitor the unused main memory of server or the available hard disk space or the percent usage of a router's CPU.

The GET command format to receive short message is:

<Community Name> GET <IP Address> <MIB Name>

And the SET command format to send short message is:

<Community Name> SET <IP Address> <MIB Name> <Command>

There are numerous numbers of MIBs and thus a subset of MIB's names and their descriptions have been depicted in table 2.

Network administrator must always have a table of MIBs applicable to the network under his domain handy. e of the important aspects of this work is the fact that this system allows network administrator to exploit full potential of the SNMP protocol while can enjoy full access to all network devices without need to access to Internet or having physical presence at the network site.

V. SECURITY ASPECTS OF PROPOSED SYSTEM

A number of steps have been taken to prevent an unauthor-ized access to the network or miss use of administrator's privilege to control overall network functionality.

TABLE II. BRIEF DESCRIPTIONS OF SOME MIBS

Description	Name	MIB
Physical Location of Node	sysLocation	.1.3.6.1.2.1.1.6
Name accompany Domain	sysName	.1.3.6.1.2.1.1.5
Period of System Uptime	sysUptime	.1.3.6.1.2.1.1.3
OS and Hardware Specification	sysDescr	.1.3.6.1.2.1.1.1
Number of Interfaces	ifNumber	.1.3.6.1.2.1.2.1
Speed of Interfaces	ifSpeed	.1.3.6.1.2.1.2.2.1.5
Interface Physical address	ifPhysAddres	.1.3.6.1.2.1.2.2.1.6
Interface Status	ifAdmnStatus	.1.3.6.1.2.1.2.2.1.7
Value TTL Defaultin IP Header	ifDefaulTTL	.1.3.6.1.2.1.4.2
Numbe of Total r Received ICMP	icmplnMsgs	.1.3.6.1.2.1.5.1

1) Database Security: Prevention of database unauthorized access is done by utilization of information hiding methods. In addition, backup procedure has been implemented in regular intervals.

2) Application Program Security: The application program has been implemented as an operating system's service. This means direct access by any user has been prohibited and with the capabilities of Windows 2003,

access to the application program files are limited.

3) Access Level Security: These days large scale networks can not be managed by one person and thus each administrator has a limited domain of network control. The application program is capable of granting access right to each individual for only a specific domain of network.

This provision of security grantee unauthorized access to different section of network is prohibited. The access right of network administrators can be redefined at any time if is required. The report generating capability of the application allows monitoring each administrator actions. For example it can be observed that what has been the response of an administrator to an event of network failure and what action has been taken on his part. To ensure the accuracy of reports, the events are time stamped and all messages are recorded in database.

VI. EVALUATION OF PROPOSED SYSTEM

The proposed system has been implemented initially in the Yazd University network lab at the department of computer engineering, under real network operating conditions. The lab network configuration which was used as a test bed is shown in Figure 3.

The application program was installed on the C1 work station with Window Server 2003 operating system. The GSM modem is also connected to the C1. The rest of the configura-tion set up were S1 and S2 as Cisco 2950 switches, R1 and R2 as Cisco 2600 routers, C2 as an work station with Windows XP operating system, C3 work station with SUSE Linux 10.0 operating system, and the server with Windows Server 2003 operating system. Two community names were created for all

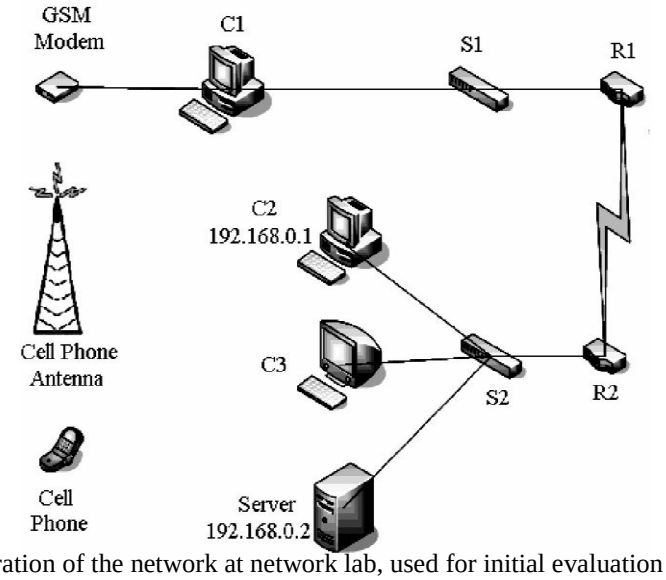

Figure 3. Configuration of the network at network lab, used for initial evaluation of proposed system

Routers and switches as “public Test” with read only access and “Private Test” with read/write access. Then the SNMP service was activated for all devices of the network. In order to establish access security to the application program, two mobile phone numbers were assigned and granted access right to communicate with the application program.

The first mobile phone number was set to access “Public Test” community and the second one was given the access to the “Private Test” community. The application program was set in such a way that could handle and respond and transmit warnings to both network administrators for the names and IP address conflict, communication link failure due to power cut, a network device power down or communication link cutoff. A name for both work stations C2 and server selected as “Test”. Upon this assignment both administrator were notified the name conflict. The first administrator could not be able to rectify this fault due to access to the read only community. Even if he knew the community name of type read/write, still he would not have been able to correct the name conflict due to mobile phone number access right. However the second administrator was able to send the following command, using the GSM modem phone number and to change the C2 work station name from “Test” to “Exam”.

PrivateTest SET 192.168.0.1 SetName Exam

In response to the above command, a confirmation message is received. Further command is issued to examine the success of previous command.

PrivateTest GET 192.168.0.1 SysName

The response to this request from the second administrator was a message which contained "Exam".

Then the R2 router was turned off for further evaluation of the proposed system. Due to this event, five messages were transmitted to both administrators. These messages indicated

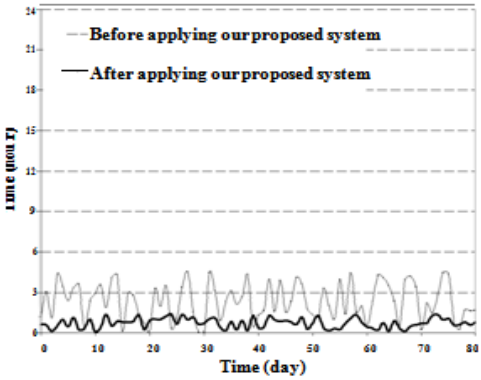

Figure 4. Comparison of statistics of downtime period of Yazd University

That R2 router, S2 switch, C2 and C3 work station were not accessible.

Following the successful initial train, the system has been installed and applied on the network management system of the Yazd University network and several accesses level for five different administrators were defined, to enable them to apply commands and to receive various reports.

The performance of this work has been monitored for over 80 days. The results have been captured using NetFlow [11 and 12] report generating application and compared with similar period in past. The statistical data shown in figure 4 indicate that our proposed system has reduced the network downtime events from 10 percent to 3 percent. The only reason to justify such improvement is the administrators' quick access to network status and speedy ramification of any network device failure.

VII. INTRODUCTION TO THE RELATED RESEARCH WORK

So far many application programs have been produced to facilitate the task of network management and control. The common approaches are those applications to report failure events to network administrator such as voice warning, Email or short messages. One of the most popular application programs is the "What's Up Gold" network management software [13]. This software can transmit a short message to network administrator upon a failure event, but it is not able to transmit a control command back in the short message format. Consequently no further request for detail of failure is possible. Therefore physical presence or access to Internet to rectify the fault is unavoidable.

VIII. CONCLUSION

In this work we proposed an overall remote management and control system for computer network administration, with utilization of short message service. The main advantage of SMS is the convenience and efficiency of having access to the monitoring and control, using the popular and handy apparatus of mobile phone. In this work we have taken the advantages of short message service and integrated with SNMP protocol by creating a middleware, referred to it as application program. This system is capable of generating appropriate report on network status and transmits to the network administrators in SMS format. It is also able to apply any necessary command, remotely by mobile phone, using SMS to control and to take corrective action on any device within the network of under administration. To provide network access security, various access levels is implemented in the application program. Thus a large network under several network administration domains would not have demarcation problem. The proposed system was utilized as a trial at the computer engineering department's network laboratory. Upon successful trial under the lab condition, the system was installed and integrated to the management system of Yazd University computer networks. Under the live network condition, the performance of the new system was evaluated over an eighty days period. This extensive evaluation showed

that not only the network downtime can be reduced, but the convenience of access to the network devices independent of place and time, i.e. without need for physical presence or access to the Internet is highly appreciated by network administrators. There is no doubt that foundation of this work can be extended for different areas of communications as in this work with SNMP protocol.

REFERENCES

[1]. D. Harrington, R. Presuhn and B. Wijnen, "An architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", RFC 3411, 2002.

[2]. R. Presuhn, "Version 2 of the Protocol Operations for the Simple Network Manag. Protocol (SNMP)", RFC 3416, 2002

[3]. M. Rose, "SNMP over OSI", RFC 1418, 1993.

[4]. U.S. Warrier, L. Besaw, L. LaBarre and B.D. Handspicker, "Common Management Information Services and Protocols for the Internet (CMOT and CMIP)", RFC 1189, 1990.

[5]. Rio de Janeiro and Brazil, "A Study of the Short Message Service of a Nationwide Cellular Network", 2006.

[6]. M.T. Rose, "Convention for defining traps for use with the SNMP", RFC 1255, 1991.

[7]. R. Presuhn, "Management Information Base for the Simple Net. Management Protocol (SNMP)", RFC 3418, 2002.

[8]. J. Case, K. McCloghrie, M. Rose and S. Waldbusser, "Introduction to Community-based SNMPv2", RFC 1996.

[9]. S. vogioukas, m. Roumeliotis, "A system for basic-level network fault management based on the GSMshort message service (SMS)", IEEE International Conference on Communications, 2001.

[10]. "AT COMMAND REFERENCE", Gtran Wireless Inc, Available at: http://www.cdmas.cz/files/, 2003.

[11]. B. Claise, "Cisco Systems NetFlow Services Export Version 9", RFC 3954, 2004.

[12]. "Cisco IOS NetFlow Configuration Guide, Release 12.4", Available at: http://www.cisco.com/application

[13]. "What's up gold Network management application", Available at: http://www.whatsupgold.co.uk/ 2006–7.