International Journal on
“Technical and Physical Problems of Engineering”
(IJTPE)
Published by International Organization on TPE (IOTPE)

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

March 2010 Issue 2 Volume 2 Number 1 Pages 60-65

NEW SOFTWARE TOOL FOR MANAGING THE PERFORMANCE OF LANS

I.M.M. El-Emary

Faculty of Information Technology, King Abdulaziz University, Jeddah, Kingdom of Saudi Arabia
omary57@hotmail.com

Abstract- All LANs require regular administration and management in order to function efficiently and effectively. A Network Administrator is required to perform a range of duties in order to achieve this efficiency and effectiveness. These include maintaining system security, implementing backup strategies, installing software, upgrading software, managing data storage and ensuring provision of virus protection. Accordingly, the main purpose of this paper is to provide an enhanced software tool used for troubleshooting the local area network. The proposed package helps the network administrator or troubleshooter to allocate, isolate and repair drawbacks that might occur in the network. Also, the proposed software has a capability of: detect any link that might go down through the use of basic or advanced "ping" commands, trace the router of packets to a specific host through the use of advanced "trace route" command and monitor all nodes and hosts in the LAN report and log any error that might occur to the link of the node or host. So, applying our suggested software tool support the major jobs of the LAN administrator. Finally, this paper was terminated with some important recommendations deals with various urgently points to be searched by others as a future work.

Keywords: LAN, Software Tool, Managing, Troubleshooting.

I. INTRODUCTION

Network management is one of the most important issues in modern communication networks. Although the concept is not new, there are still many unsolved issues. The majority of network management systems (NMS) use simple network management protocol (SNMP) standardized by IETF [6]. According to the TCP/IP reference protocol model SNMP is an application layer protocol. It relies on transport protocol UDP, and as its name says, it is a simple protocol.

The main idea is that SNMP messages must be short and they should not saturate the network. Network management station runs network management application (NMA) and is called a manager [6]. All other networked devices, such as PCs, workstations, routers, switches etc, are agents, running network management entity (NME) responsible for collecting management data. Manager polls agents and collects the data. SNMP supports three different commands: Get, Set and Trap.

Using Get command manager collects data from agents. Set command enables to a manager to change values of different variables in agent’s management information base (MIB). Finally, agents use Trap command to warn a manager that something important is going on. Accordingly, a manager should do some action using Get and Set. Hence, on the protocol level everything seems quite arranged and well defined. But, on the network management application level things are different. There are many products on the market, but it is really hard to find software that is very well suited to network management needs. One of the most important NMAs is Open View [7].

It is huge, powerful software, full of functionalities, but it is also very complex for use and maintenance. The computer network technology has rapidly grown into a widespread, fundamental building block for information exchange. As communication technology becomes increasingly important, there is growing pressure to use this technology to reduce costs without sacrificing any capabilities or benefits Local Area Networks (LAN) are data communication network used for connecting network devices over a relatively short distance. An important feature of a LAN is its topology, where the term topology refers to the layout of connected network devices on a network. Network topologies can be categorized into the following basic types: the bus, the ring, the, star and the star wired ring topology.

In this paper, we introduce the basic components of computer network management and monitoring as well ns the various protocols and utilities used in the managing and monitoring processes. Also presented in our work, some of the management standards and monitoring techniques by which the network administrator can verify reliability as well as achieving the goals of the optimum performance for the network. So, when we discuss this point, we should cover the topic of computer network management protocol which was designed to help maintain a steady and reliable network capable of adapting to various changes in the surrounding environment. Simple Network Management Protocol (SNMP) and Remote Monitoring (RMon) are the two most famous and powerful network management protocols [1, 2].

Finally, described in our paper, the various reasons that might be behind any kind of failure or drawback Cable cuttings or disconnection, and IP addresses arc some of the most common network problems. Get to know how to detect, diagnose, and fix any errors, or problems that might occur in the network using a hierarchy of steps and algorithms.

Survey more about the most common and widely used troubleshooting techniques that have been developed throughout the history of computer networks to serve as the ultimate guide for network troubleshooting. The main contribution that has been described and clarified well is our implementation software that is used in managing and troubleshooting process. This software was coded in order to simplify the process of managing a network using the simplest yet most important management functions "Ping" and "Trace Route", The was terminated with the results of various tests implemented using the management software included (NetMOn viI.G) along with a set of conclusions and suggested continuation work.

II. NETWORK PERFORMANCE MONITORING

In many situations stuff that manages some network needs only a small software packet for network monitoring, without advanced features, like NMA user administration, network topology discovery etc. A typical example of network monitoring tool is MRTG [8, 9]. It simply collects network management data and produces desired graphs presenting network performances. MRTG is a good management tool but in some situations its performances could be quite limited. Let us presume that a user wants to manage a local area network (LAN).

If MRTG is installed on a workstation in a local network, everything looks fine. But if a user wants to access to a local network via Internet, things change. There are many examples where a person monitors several LANs on different locations. In that situation he is forced to access these networks via Internet. The only way for monitoring application to collect data is to permanently send Get commands to these LANs. And that is where the problem arises.

The more LANs have to be monitored the more Get commands should be sent to different locations. Accordingly, the period between two consecutive Get commands sent to the same LAN is bigger and bigger. Second problem is tied to a response time. Sometimes Internet can become quite saturated.

NMS sends Get commands periodically in regular time intervals. But there is no guarantee that these commands will reach a target in the same order. Furthermore, responses from managed network devices travel back to NMS. It is quite possible that some UDP packets carrying SNMP data can be lost or suffer from high delays.

III. LAN MANAGEMENT AND MONITORING APPROACHES

The task of maintaining and monitoring a network is to make sure that all programs are up to date, all functioning properly and all authorized users are able to access and work on the network is what, is, so called Network Administration. So.-the duties of the administrator or manager of the network Fall into the following: (1) Setting up new accounts: (2) Assigning user privileges, permissions, and so on; (3) Billing and other accounting chores; (4) Testing and illustrating new software or hardware; (5) Troubleshooting existing hardware and software; (6) Backup and file management [3].

Network performance management is one of five OSI network management domains specified by the ISO. This domain is concerned with the following: 0) Monitoring the day to day network activity, (2) Gathering and logging data based on this activity, such as utilization, throughput and delay values; (3) Storing performance data as historical archives to serve as a database for planning network optimization and expansion; (4) Analyzing performance data to identify actual and potential bottlenecks, and (5) Changing configuration settings in order to help optimize network performance.

The above first two, points address the data-collection capabilities expected of a performance management package. The next two points concern data-analysis capabilities that are used to plan interventions. The last point relates to the control such that a package can exert to change a network's performance (data-control). Sophisticated packages can apply control directly; simpler packages require the system administrator to make the actual changes (i.e. manual interference) [10].

There are many ways in which data can be gathered, and by which careful thought must be given in selecting the most appropriate methods for ones needs. Data collection may use one of the following methods:

a) Snapshot approach, in which values are taken at a single instant in time. This approach is listed most commonly when troubleshooting or when gathering rough;

b) Statistical approach, in which the management component looks at network activity at periodic or random intervals;

c) Exhaustive approach, in which the networks activity is monitored constantly.

Many performance indicators may be viewed form multiple perspectives and using different measures commonly used measures include: frequency, relative frequency, duration or delay. If a performance indicator approaches or exceeds a threshold value, the performance-management package may take action. This action may be as simple as giving an alarm to call the indicator level to the system administrator's attention. At the other extreme, the management package may change one or more configuration settings. Interventions and changes in configuration values are likely to be made through the configuration management.

IV. NETWORK MANAGEMENT PROTOCOLS AND UTILITIES

A management protocol is software that contains previously gained knowledge of the structure of the network. Its job is to fully monitor and control all managed network devices. SNMP (Simple Network Management Protocol) itself is a simple request / response protocol, NMSS (Network Management Stations) can send multiple requests without receiving a response [4]. SNMP started to work on traditional test message from the ICMP (Internet Control Message Protocol) protocol, and when was developed to use more complicated commands to achieve more goals in network monitoring.

SNMP protocol architecture is divided into three major parts: Managed parts, Manager, Agents and Management Information base. SNMP V1.0 messages contains two parts, the first is a version and a community name and the second in actual SNMP protocol data unit (PDU) specifying the operation to be performed. SNMP V2.0 messages contain two parts;, the first part contains the majority of the difference between SNMP V1.0 and SNMP V2.0. The second part is virtually identical to that of an SNMP V1.0 message. To help ensure message privacy, the Symantec privacy, protocol is used as a secret encryption key known only to the sender and the receiver.

Remote Network Management (RMON) technique defines remote monitoring MIB that supplements MIB-II. RMON can not easily learn about LAN traffic as a whole, and so that it cannot obtain information and results that is purely local to individual devices; RMON MIB contains several groups, which are: Statistics, History, Host, Matrix, Filter and Capture.

V. DESCRIPTION OF LAN TROUBLESHOOTING APPROACH

The determination of LAN: A problem is the first step make in order to start troubleshooting any problem in the network. Most problems in LAN happen in the physical layer, 90% from LAN errors occur in the cabling system in the LAN. Error in the lager 2 is mainly concerned with the configuration of the Ethernet cards, or encapsulation errors caused by using different encapsulation types. Layer three errors occur because errors in assigning the IP address or sub net Mask. [5, 6]. Errors may affect all users in the network, or some of the LAN users are affected according to the error that causes the network problem. A layered approach to the problem must be implemented in handling LAN problems. The person at the help desk is the first level of repairing; he interacts with the user to determine the nature of problem, by using a standard set of questions. Also, the troubleshooter can use the ohmmeter, time domain ref meter and voltmeter as basic cable troubleshooting tools. Different LAN topologies implement different troubleshooting steps, according to the different errors that may happen to the LAN. As for troubleshooting, methods, Divide and conquer and process of elimination are the most common troubleshooting strategies used in LAN troubleshooting.

VI. PROPOSED SOFTWARE PACKAGE FOR LAN TROUBLESHOOTING

Our suggested software was coded using Microsoft Visual Basic v6.0, serves as a simple network monitoring tool which the network administrator can uses a first step in identifying a faulty node or drawback in the network, should it occur. Our program is based on the two most simple yet vital network commands used in verifying connectivity, accessibility and signal quality, "Ping" and "Trace Route". By creating a ping or trace string, the program can monitor and tack down any host available in the program database, and return results concerning the state of the link to that host, whether it's up or down. Also the delay in a functioning link is viewed. All test and operation results are saved in log files for future reference or study. Through these log files, statistical information can be made for the use in assessing the network state, and therefore, the administrator can determine what act(s) should be done, and where to do them, in order to verify the networks reliability as well as its performance. Ping is a utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connection. There are many freeware and shareware Ping utilities available for personal computers ("Ping" is an abbreviation for "Packet Internet Griper").

Trace Route is a utility that traces a packet form your computer to a host, showing how many hops the packet requires to reach the host and how long each hop takes. The user can use trace route to figure out where the congest delays are occurring in a network. The original trace route's a UNIX utility, but all platforms have something similar. Windows Includes a trace route utility called tracer. Trace route utilities work by sending packets with low time-to live (TTL) fields. The TIL value specifies how many hops the packet is allowed before it is returned. When a packet can't reach its destination because the TIL value is too low, the last host returns the packet and identifies itself. By sending a series of packets and incrementing the TTL value with each, successive packet, trace route finds out who all the intermediary hosts are. One of the advantage of the presented software is that is uses a graphical interface to generate the ping or trace command rather than the .traditional MS-DOS interface This is done by entering some host-related information into text fields and clicking a single button to get the results. This also proved its efficiency from the concept that any ordinary user can apply the ping or trace commands without knowing the exact command line syntax. Each input test field is subject to a validity test. If the input is invalid, a message box alert will appear telling the user to change the contents of that field. This comes according to the specified international standards of the ISO and CCITT committees. These standards identify a set of rules and value ranges for IP addresses, data packets size, number of packets sent, time to live (TTL), request timeout, and number of hops. The main flowchart that describes our software is shown in Figure 1. For the continuation points shown in Figure 1 labeled

from CI to C7 we define these points as:
C1: Wait for an input, and then add new host followed by the same steps executed in the main Screen from search till the exit.
C2: Checking about the clicking of the NetMon v1.0.
C3: Inserting a host name, IP address, and PC type; also checking the validity of the IP address and if the valid and selected IP address exists in the database or not.
C4: Checking about the IP address to search for an examining the existence of data in the Database then asking some queries as: edit. Delete, ping, trace, Ok, cancel back, ping log trace log.
C5: Checking the successfully of the transmitted ping in order to update the lists of success and fails and charging the settings then asking to create log to assign path to save log file.
C6: Checking either all fields are filled, validity of echo number, validity of TTL, packet size, or view log clicked.
C7: Checking either all fields are filled, validity of hop number, create "Trace" command, creating a log Ad Trace, saving ping results in the trace log file, and finally checking about log clicked.

VII. SIMULATION RESULTS

In this section, we present the statistical results of some tests run using the implementation software (Net Mon vl.0). The test covers listing of all graphs that resulted from the various tests applied on different numbers of PC's at different time intervals using difference packet as request signals. The next Tables 1, 2 and 3 and Figures 2, 3 and 4 show a comparison in the average delay in a network of 30 PC's using various packet sizes at different time intervals (from 9:00 am till 4:00 pm). From these three figures, we notice that the larger the packet size sent, the larger the average delay becomes. This means that we have a directly proportional relation between the packet size sent and the average delay in a network. The next Table 4 and Figure 5 shows a comparison in the average delay on the same computers tested earlier with the change in the cable speed with single and duplex path using a packet size of 32 bytes. From this Figure 5, we notice that the cable with single speed and duplex play a major role in the total average delay time in a network. When using 10 Mbps half. Duplex cables the average delay is relatively higher than the delay in the other three cases. This is due to the-reason that the PC can send and receive signals at the same time, and cases because the cable speed is less. The average delay using 100 Mbps using full duplex cables is low in comparison with the two other types. We conclude that the amount of average delay is inversely proportional to the speed of the cables, which means, the higher speed the cable is, the less average delay occurs.

VIII. SUMMARIES, CONCLUSIONS AND FUTURE WORKS

This paper sheds the light on the importance of LAN management in: maintaining a steady and, efficient Work. Also, 1 this, paper presents various contributions represented by:
(1) Improving the out screen to be more User-friendly and modem rather than the traditional Ms-DOS black output screen;
(2) The user can execute "Ping" and "Trace 'Route" commands without the' need' to be fully aware of the exact command line that should be' used, instead; the of the' post is enough;
(3) The capability to ping more than one host at a time using a single; button Click, without the need to' issue a separate ping command' for each 'and every' host.
(4) Creating "log" files in which the "Ping" and "Trace: Route" results are saved for, future reference;
5) The ability to print out the ping and trace results on, paper with a single button click.

As a future work to the above, we recommend executing the following search points: The implementation of an experts system that can be installed on each station on the network, which will give the station the capability of managing and troubleshooting itself, and also trying to fix problems, unless the problem needs human efforts to be fixed (broken or damaged cables). The system is capable of troubleshooting logical problems concerning layers two errors and above. The system can be implemented using a layered approach troubleshooting strategy, starting form layer two and moving upwards in the layers of the OSI model. This expert system will help reduce human effort concerning layers two and above troubleshooting. Add a new option in the NetMon software named "Mailing list", this option is designed to store a number of e-mail addresses. The list of addresses is to be notified of any drawback or failure that occurs in the network by sending a warning e-mail to all the e-mail addresses on the list. Adding such an option will be helpful to notify the LAN administrator and other top Management members of important link that might go down so as to fix problem or soon as possible.

REFERENCES

[1] R. Mon, "Bay Networks: Overview", http:/support.bavne_works.com/library/tpu_.

[2] S. Kalyanaraman, "Simple Network Management Protocol (SNMP)", Rensselaer Polytechnic Institute, 2000.

[3] "Network Management & Control Mechanism to Prevent Induced Network Instability", The Laboratory for Telecom Sciences, 20 a1.

[4] "A Secure Station for Network Monitoring & Con_ol", USENIX Association, 1999.

[5] "Troubleshooting Your LAN", http://www.CIT.comell.edu/computer/SYOOirtitroubleshooting.LAN.htm!

[6] I.M.M. El Emary, "Developing Enhanced Software Tool for Troubleshooting and Administrating the Local Area Networks", Journal of Institute of Mathematics and Computer Sciences, Vol. 14, No. 2, Dec. 2003.

[7] "SNMP", NASA Advanced Supercomputing Division, http://www.nas.nasa.gov/Groups/LAN/ClassNotes/snmp/.

[8] S. Maxwell, "Red Hat Linux Network Management Tools", McGraw-Hill, 2001.

[9] "SNMP", NASA Advanced Supercomputing Division, http://www.nas.nasa.gov/Groups/LAN/ClassNotes/snmp/.

[10] D.R. Mauro and K.J. Schmidt, "Essential SNMP", O"Reilly, 1st Edition, 2001.

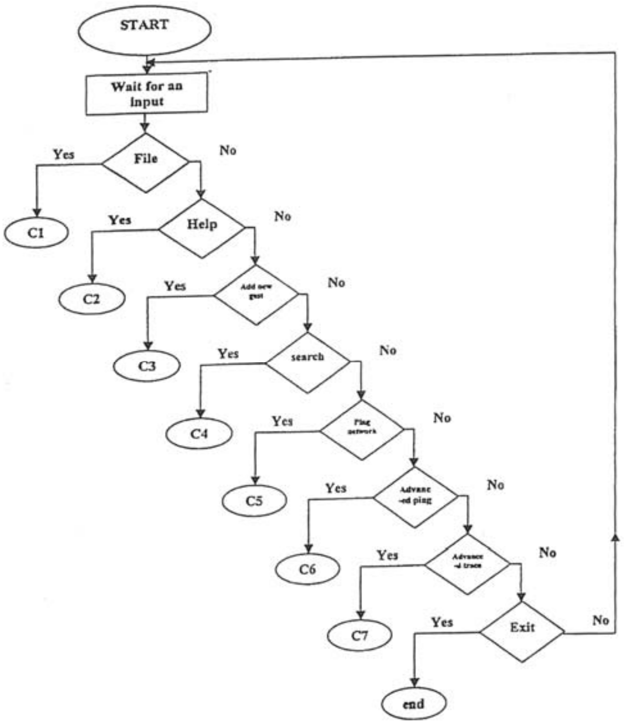


Figure 1. Main flowchart of the software used for LAN troubleshooting

Table 1. Average Delay of 30 PC

	Delay (ms)	
Time	32B	128B
9.00	0.08	0.10
10.00	0.12	0.22
11.00	0.12	0.19
12.00	0.12	0.20
1.00	0.10	0.13
2.00	0.14	0.50
3.00	0.12	0.20
4.00	0.05	0.10

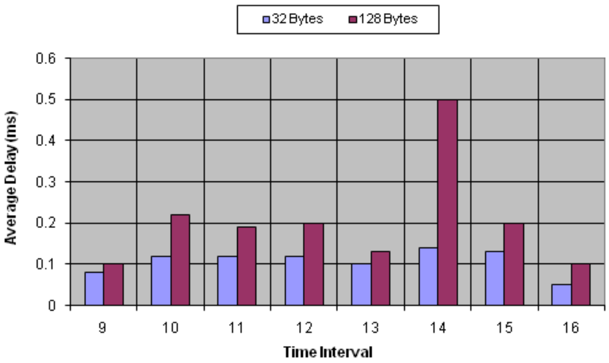


Figure 2. Average delay of 30 PC

Table 2 Average Delay for 1 far PC

	Delay (ms)	
Time	32B	128B
9.00	0.00	0.00
10.00	0.20	0.32
11.00	0.25	0.50
12.00	0.50	0.70
1.00	0.97	0.98
2.00	0.32	0.46
3.00	0.00	0.23
4.00	0.00	0.00

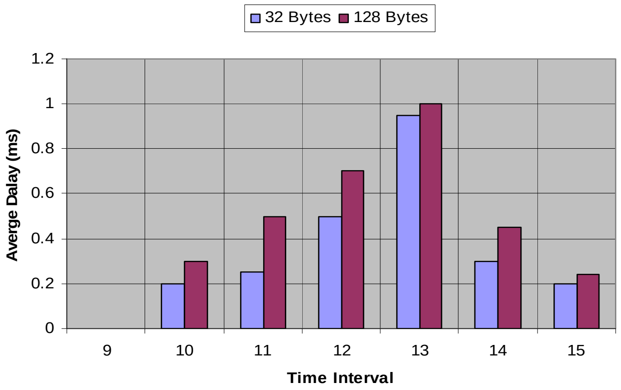


Figure 3. Average delay of 1 far PC

Table 3 Average Delay for 1 near PC

	Delay (ms)	
Time	32B	128B
9.00	0.05	0.06
10.00	0.05	0.33
11.00	0.08	0.28
12.00	0.02	0.02
1.00	0.01	0.10
2.00	0.01	0.10
3.00	0.01	0.45

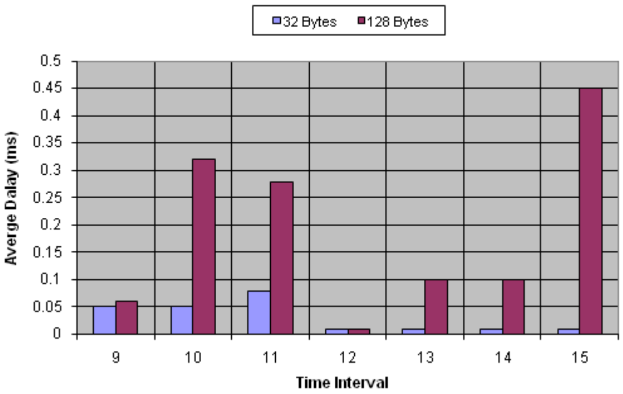


Figure 4. Average delay of 1 near PC

Table 4. Average Delay of Various Speeds

Time	10/HD	10/FD	100/HD	100/FD
9.00	0.01	0.06	0.02	0.08
10.00	0.24	0.32	0.24	0.12
11.00	0.63	0.46	0.13	0.12
12.00	0.56	0.24	0.17	0.12
1.00	0.13	0.16	0.06	0.09
2.00	0.09	0.14	0.15	0.14
3.00	0.10	0.12	0.03	0.12
4.00	0.03	0.09	0.01	0.03

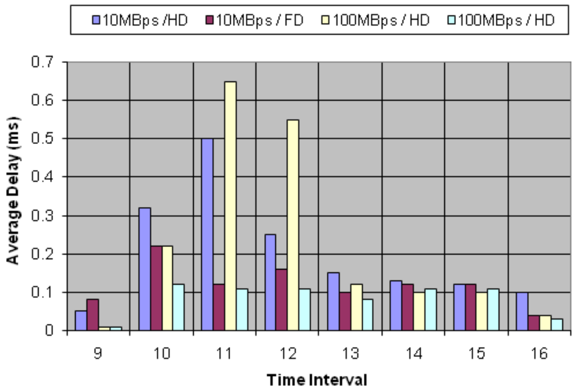
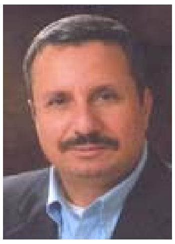


Figure 5. Average delay of various speeds

BIOGRAPHIES



Ibrahiem M. M. El-Emary received the Dr. Eng. Degree in 1998 from the Electronic and Communication Department, Faculty of Engineering, Ain Shams University, Egypt. He is a visiting Associate Professor in faculty of Information Technology, King Abdulaziz University, Kingdom of Saudi Arabia. His research interests cover: analyzing the various types of analytic and discrete event simulation techniques, performance evaluation of communication networks, application of intelligent techniques in managing computer communication network, and performing comparative studies between various policies and strategies of routing, congestion control, sub netting of computer communication networks. He published more than 70 articles in various refereed international journals and conferences covering: Computer Networks, Artificial Intelligent, Expert Systems, Software Agents, Information Retrieval, E-learning, Case Based Reasoning, Image processing, wireless sensor networks and Pattern Recognition. Also, in the current time, he is too interested in making a lot of scientific research in wireless sensor networks in view point of enhancing its algorithms of congestion control as well as routing protocols. Also, he is an editor in chief of two international journals and associate editor of more than 10 international journals.