(IJ-02) Network Monitoring System

Dr. Shams Al Ajrawi
San Diego State University, 5500 Campanile Dr, San Diego CA 92182

Ali Rasouli
San Diego State University, 5500 Campanile Dr, San Diego CA 92182

David Kelble
San Diego State University, 5500 Campanile Dr, San Diego CA 92182

ABSTRACT

It is vital to the security and management of the network to have a network monitoring system in place.

Observation of network events is needed to provide a safe and reliable network. The goal of network monitoring is to secure and maintain the network. Despite this, many small and medium-sized businesses and organizations prefer to ignore this fact. Such companies cannot use the available network monitoring system because they lack the skills of professional network administrators. This avoidance would cost them a significant amount of money or even cause them to fail financially [4]. Due to its ease of use and ability to provide all the necessary functionalities for monitoring a network, the network monitoring proposed in this report will fix this problem. It would therefore be advantageous for users of the proposed system to be able to use it even if they are novices who have only rudimentary knowledge of computer applications. Hence, Small and Medium-Sized Businesses can use this application if they are not equipped with professional network administrators.

INTRODUCTION

A room-sized computer, which was invented many years ago, had a standalone processing unit that could perform some simple calculations. The first computer was invented more than 30 years

ago, and since then, computers have improved greatly. These days, the biggest challenge is connectivity for this technology. In recent years, almost every simple office has a plethora of machines, printers, scanners, server and so on. It is common practice for even personal computers to be connected to other computers, smart home systems, and such from a private place. Networks are responsible for providing the mentioned connectivity. The ease of communication, transferring, and connecting has been greatly facilitated by networks. The Internet has evolved from connecting a few computers through the years to connecting many computers through multiple networks due to advances in technology. Having a rich management system would be necessary for this complex network. Since the formation of the Internet, network management has become a necessity [5]. Monitoring and controlling how a network and its devices are connected is called network management. As part of network monitoring, devices in the network will be checked for connectivity, malicious activities will be checked and detected, and many other tasks will be handled, with the goal of providing a healthy network with high performance. Network management might not be a considerable issue for a small network, such as a home network. A high-performance and smooth network is, however, a priority for large organizations. An organization can lose even a large part of its profit and go bankrupt if they do not have good network management. Some organizations, such as banks, airlines, libraries, and so on, can be considered to have networks that are so complex that if they encountered problems with their network, they would not be able to provide services to the customers. Whenever an organization says it is going to provide services for its customers, they must keep their network up and running [1] [2]. Thus, nowadays, networks that are smooth and healthy are of utmost importance in organizations. Organizations need to manage their networks effectively in order to accomplish this goal.

DESCRIPTION OF THE PROJECT

A Network Monitoring System has been implemented for this project that monitors the network by issuing a ping command and logs the ping result and faults if any. A host's reachability on an IP network can be tested using this application. A specific IP address or host name is requested by the application over the network. Upon successful ping, a response is returned from the originating computer to the one that initiated the ping.

EXPERIMENTS

The Networking Monitoring System application is written in Visual Basic and it utilizes 3 windows forms. The first window form is the Main form which allows the user to input an IP address or a destination host name. See Figure 1. Window 2 is the log window which shows the ping results and errors/faults if any (Figure 2), and window 3 is the About window that shows the revision of application and credentials (Figure 3).

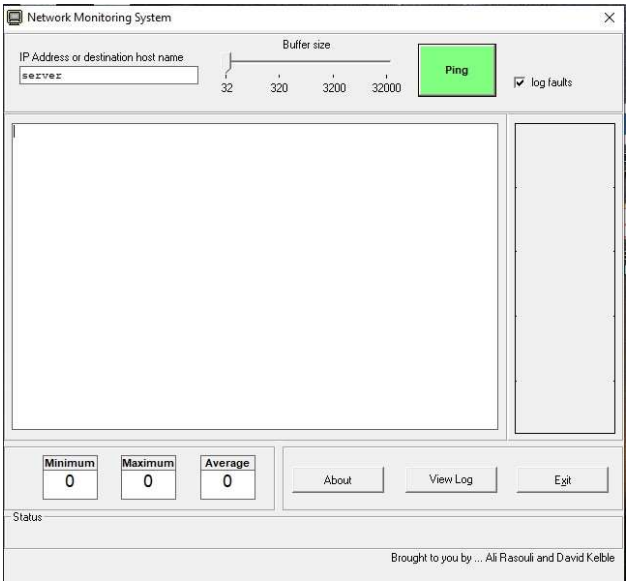

Figure 1: Main window

The user has the option to choose from 4 different buffer sizes (32, 320, 3200 and 32000 bytes). The application allows the user to select if fault logging is enabled or not. If enabled, all faults will be logged on the local hard drive. Once an IP address or the destination hostname is entered, the user will click on the Ping button. The application then tries to ping the IP/hostname. In the center of the window, the application shows the ping in process, while on the right-hand side box it shows a bar graph of how fast the ping is being returned. Also, in the lower part of the application, the ping process is shown in 3 different boxes as Minimum, Maximum and Average. See Figure 2.

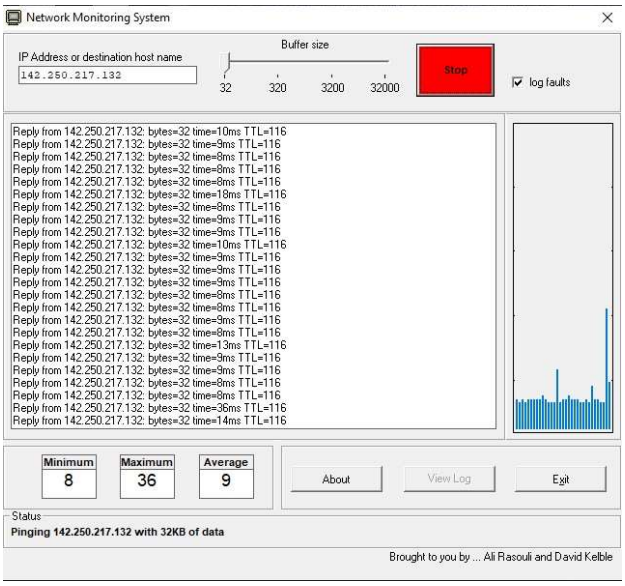

Figure 2: Ping in process

If successful, it would then log the result in a text file that is saved locally. If the ping fails it would then document the result into the fault log file. The user can click on the

"View Log" button in the lower right part of the main window to display the "log" window. The "log" window then shows the ping result on the left part of the window and the error result on the right-hand side. The user can clear both log files by clicking on the "Delete log" button on the lower left-hand side of the "log" window. The user can close the application by clicking on the "Exit" button on the main window.

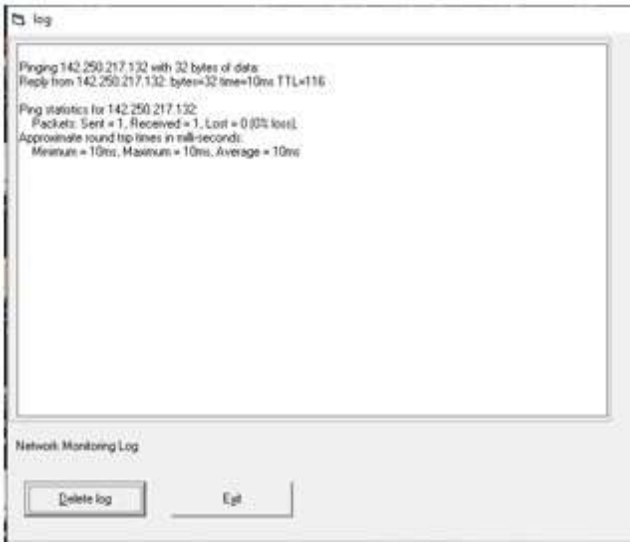

Figure 3a: Log Window

Figure 3b: Log Window

By clicking on the "About" button on the main window, the user can display the general information about the application and the credentials

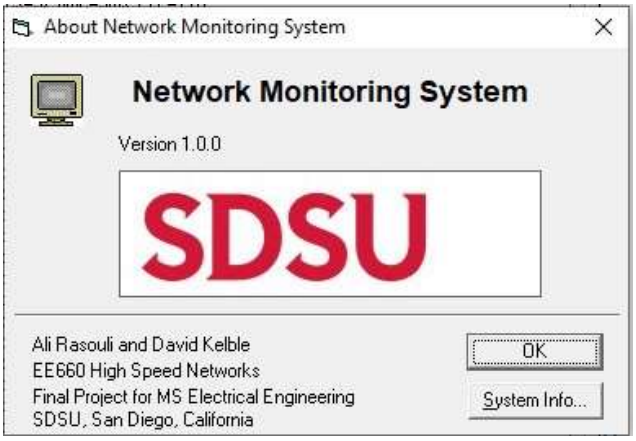

Figure 4: About window

SIMILAR WORKS

The next part of the article reviews similar network monitoring applications to that proposed here. The following softwares will be discussed in detail, along with their pros and cons, in order to provide some familiarity with them.

All manuscripts must be in English.

1. Wireshark

This article will describe how Wireshark can be used to monitor and analyze networks with its simple and intuitive interface. This is a popular and comprehensive tool that gives users the ability to easily analyze packets, Voice over Internet Protocol (VoIP) analysis, traffic monitoring, and a great deal more using Wireshark." By capturing packets in your network, this application allows you to analyze them and save them the way you want. Both the advantages and disadvantages of this tool can be found in the following list. The cost-free nature of the software, the fact that it is open-source, and the fact that it can run on any operating system can all be considered as some of its strengths. Even though this packet analyzer is an amazing tool, it has a difficult-to-use interface. Moreover, Wireshark requires that you have a comprehensive knowledge of Protocol Control Protocol/Internet Protocol (TCP/IP).

2. Spiceworks

Spiceworks is also a popular network monitoring tool.

Monitoring events in the network is possible with this tool. A feature of this tool is that it analyzes network performance and bandwidth. With this software, the administrator can control network configurations as it comes with an in-built server. Furthermore, Spiceworks gives administrators access to information about connected devices and to their data, as well as their accounts. Moreover, administrators could answer any requests for network administration from the workstations. Despite Spiceworks being one of the most powerful and simplest network monitoring systems around, you cannot run it on Linux based operating systems. Spiceworks also lacks the ability to grant its users the ability to control the network and the user can only view the network activity on the monitored network [3].

CONCLUSION

By conducting this study, various concepts related to this work, including network monitoring, remote access, and other systems related tools, had been explored. Additionally, we compared our developed tools with the existing tools that had been used previously in this field, and investigated similar works that were done previously. A simplified network monitoring system was developed within the scope of this project. All the existing network monitoring tools on the market, if they don't work using command line structures, have complicated user interfaces based on the research done prior to choosing this topic. Because of this fact, the existing tools are not designed for beginners and are meant for expert users who have a strong understanding of networks. The primary objective of this project was to provide a network monitoring system that is easy to use. Aside from these purposes, the proposed system's main focus is on the networking security and management aspects as well as monitoring user behavior. The admin of a user will have the ability to control the security of the entire network through monitoring and sniffing packets. This project implements a network monitoring system that is capable of being used by novice computer users as well as students. This creates the possibility of using the application for educational and training purposes. It is possible to keep adding more features to this application in the future, such as generating statistical reports on the results of the monitoring and transferring data, which can be done by using File Transferring Protocol (FTP), so as to support the future improvement of the

application. Furthermore, the application, which was originally intended to be run on windows operating system, may also be written in another programming language so that it can be used on devices other than Windows operating system.

REFERENCES

Gordon Fyodor Loyd, (2008), Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security.

Stephen, P., Olejniczak & Kirby, B., (2007), Asterisk for Dummies, chapter 10.

Malay Kumar Kundu, Durga Prasad Mohapatra, (2014) Advanced Computing, Networking and Informatics- Volume 1: Advanced Computing and Informatics.

Nikolas Mitrou, Kimon Kontovasilis, George Rouskas, Ilias Iliadis, Lazaros, (2004), NETWORKING 2004: Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks

Easley, D. & Jon Kleinberg, (2010), Networks, Crowds, and Markets: Reasoning About a Highly Connected World.