Implementing Network Monitoring Tools

V.C.Asiwe and P.S.Dowland

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

One very vital tool for networks is the network monitoring tool. These tools are part of the network because of their role in allowing administrators to observe and analyse the network at any time. This observation and analysis are fundamental to the smooth running of the network because they aid in managing network resources and ensure that the performance of the network is not hindered. This paper describes the implementation network monitoring tools that have functionality capable of performing simple monitoring tasks as well as packet capturing. The tool was designed and implemented under a Windows environment and it was designed to be user-friendly and simple while at the same time providing user with enough functionality for monitoring their networks. The effectiveness of the tools implemented was evaluated with the aid of a survey and the results analysed shows that it meets it requirement specification.

Keywords

Networks, Network monitoring, Network monitoring tools, implementation, survey

1. Introduction

Networks evolved out of the need for sharing information and for communication between two or more computers. As these needs increase, networks grew in size, operational cost and complexity. Presently the size of a network can span the globe and can be as complex as having many networks connected together as a single network. The operational cost involves service interruption as a result of abnormal conditions and failure of a network device. This growth in turn presented severe problems because many organisations could not justify the use of the network as a result of the poor Return on Investment (ROI) recorded. The first step in the solution of the problems brought by the growth of the network is to monitor the network to identify certain trends and proactively solve these problems (Held, 2000; Gaglio et al. 2006).

Monitoring a network involves the use of specialized tools that can keep track of the status of all the various devices on the network; identify and analyse incoming and outgoing traffic; identify problem areas and check for certain trends by alerting the network administrator of their occurrence. These tools provide means by which the configuration settings of the network can be managed, the performance of a network can be evaluated and any faulty condition diagnosed. This research was conducted to implement a set of simple network monitoring tools under the Windows platform. The rest of this paper will be structured to give a thorough understanding of the concepts involved in the implementation. Section 2 introduces the concepts involved and detailed the approach used in creating the network monitoring tools. Section 3 introduces the research methods used in conducting this research. Section 4 introduces how the implementation of the tools was evaluated. Finally, section 5 presents the conclusions.

2. Network Monitoring Tools

2.1 Network Monitoring

Network monitoring involves observing and analysing the status and behaviour of part or the entire network that create what needs to be monitored and managed (Wisniewski, 2003*)*. Network monitoring takes place at layers 1, 2, 3 and 4 of the Open Systems Interconnection (OSI) reference model. At layer 2, network monitoring uses MAC addresses to capture frames as they enter and exit the network. At layer 3, network monitoring uses source and destination IP addresses for packet capture and at layer 4 monitoring is done using source and destination port numbers and protocols like TCP and UDP (Held, 2000; Miller, 1999). This is depicted in figure 1 below.

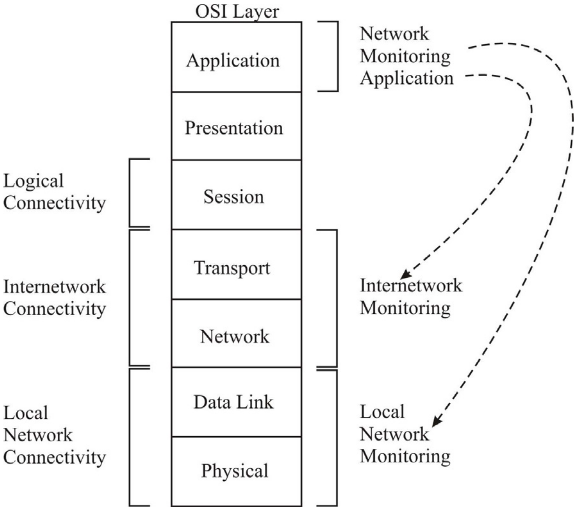


Figure 1: Network monitoring within the OSI framework (Miller, 1999)

Network monitoring is very vital to network management because a network to be managed must first be monitored. Leinward and Fang (1993) described network management as a process of controlling a complex network to maximise its efficiency and throughput. Burke (2004) noted that network management is mostly a combination of local and remote configuration and management with software. In this vein, network monitoring can be said to be a subset of network management. Liska (2003) noted that logging is a very vital aspect of network monitoring and it notifies an administrator via e-mail, telephone or Simple Message Service (SMS) when trappable conditions occur.

2.2 Network Monitoring Information

Network monitoring information can be classified into static, dynamic and statistical information. Static information is characterized by the current information, as such, it will rarely change. Static information is always generated by the various network devices that are monitored. Dynamic information is related to events happening in the network in real-time. Statistical information can be generated by network devices that have access to dynamic information. This information is collected, analysed and summarised statistically producing bar chart, pie chart, histogram and graphs as the need arises (Wisniewski, 2003).

2.3 Network Monitoring Tools

Network monitoring tools gather information about the general condition of the entire network to identify those areas that are failing and need managing. These tools can also check the overall performance of a network against a baseline taken when everything was working perfectly well. With these tools, the network administrator can observe the operation and performance of network infrastructures (Held, 2000). These tools provide network monitoring information with which the network is analysed.

2.4 An Overview of Existing Network monitoring Tools

Ping is a command line utility that tests for connectivity by checking if a destination can be reachable from a source in an IP network. It uses the sends ICMP echo request packets and listens for ICMP echo reply packets to accomplish the connectivity test (Cheswick and Bellovin, 1994; Leinward and Fang, 1993; 2006; Wisniewski, 2003). Traceroute is a command line utility that determines the route a packet takes from its source to reach its destination. Tcpdump is the most used tool for network monitoring and data acquisition. It allows capturing and display of TCP/IP packets as they are being sent and received to and from a network adapter. It allows us to precisely see all network traffic. It provides a standard packet capture interface, a common dump format, basic packet decoding features and can filter based on user specification (ComLab, 2006; IEPM Website, 1999). Windump is the equivalent of tcpdump, but used for Windows. Windump can be used to watch, diagnose and save the network traffic based on the rules the user specify (Windump, 2006). WildPackets Etherpeek is a portable Ethernet-specific network analyser that allows for visibility into every part of the network. (WildPackets, 2006).

This research implements a suite of network monitoring tools from within a single Graphical User Interface (GUI). The remaining subsections discuss the implementation of the tools.

2.5 The Network monitoring Tools Implemented

The network monitoring tools implemented by this research provide a means of gathering information from frames, packets and protocols. As with all monitoring tools, it has the capability to track outstanding problems by using administrative alerts via Yahoo! Mail when faulty or undesirable network conditions occur. As part of its functionality, it can translate between IP address and host name and vice versa, display the arp table, test for connectivity between two network devices using ping, trace the route taken by a packet to its destination, capture packets for analysis, monitor network traffic by displaying the packets sent and received on the network interface and determine the throughput of the interface.

2.6 The Network Monitoring Tools Design Approach

The design approach taken makes use of a software solution based on layers 2, 3 and 4 of the OSI model. This approach entails making the implementation user-friendly, simple while still maintaining the key features and easy to expand and customize.

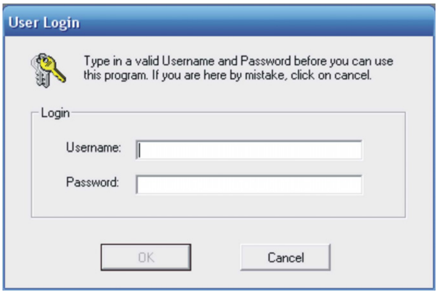
2.7 The Network Monitoring Tools Implementation

The network monitoring tools were implemented using a PC having an AMD Athlon™ XP 1.5GHz processor with a 256MB of physical memory and a network adapter as the hardware platform. The software platform for the implementation was done using Microsoft Visual Basic (VB) and Microsoft Windows XP. Visual basic was used because the systems development methodology used was prototyping and this is a Rapid Application Development (RAD) methodology and Visual Basic supports RAD. The implementation relied extensively on the use of Application programming Interface (API) and Windows socket (Winsock) programming.

2.8 Forms Used for the Implementation

The software was implemented using Microsoft VB. VB uses forms as its visual elements. The software comprises a lot of forms. The notable ones are discussed below:

Once the application has started, access can only be granted while a user is logged on. The form that handles login is shown in figure 2.



User Login

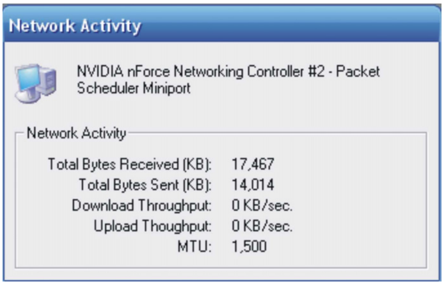
Type in a valid Username and Password before you can use this program. If you are here by mistake, click on cancel.

Login

Username:

Password:

Figure 2: The login form



Network Activity

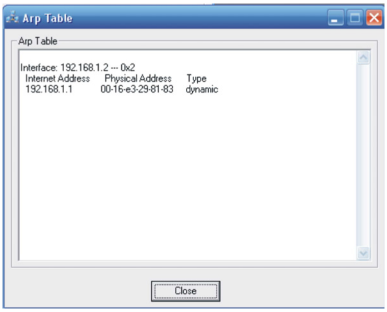
NVIDIA nForce Networking Controller #2 - Packet Scheduler Miniport

Network Activity

Total Bytes Received (KB): 17,467
Total Bytes Sent (KB): 14,014
Download Throughput: 0 KB/sec.
Upload Thoughput: 0 KB/sec.
MTU: 1,500

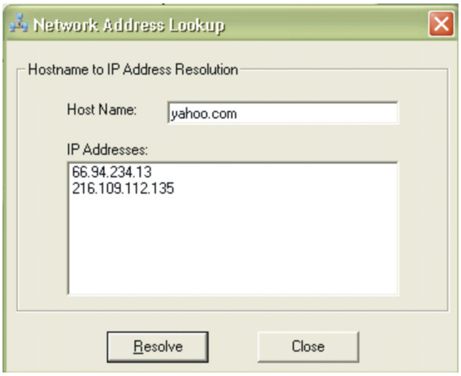
Figure 3: The network activity form

The form shown in figure 3, displays the total bytes sent and received on the network adapter and the download and upload throughput. Figure 4, displays the arp table being used by the LAN. Arp is used to resolve an IP address to a MAC address.



```
Interface: 192.168.1.2 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           00-16-e3-29-81-83     dynamic
```

Figure 4: The Arp form



Host Name: yahoo.com

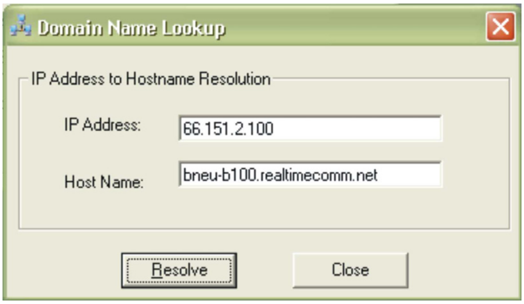
IP Addresses:
66.94.234.13
216.109.112.135

Figure 5: The network address lookup form

The form shown in figure 5 is used to resolve a hostname to an IP address. It takes as input any hostname and produces as output a list of IP addresses corresponding to the hostname.

As shown in figure 6, this form is used to resolve an IP address to a hostname. It takes as input an IP address and gives as output the corresponding hostname.

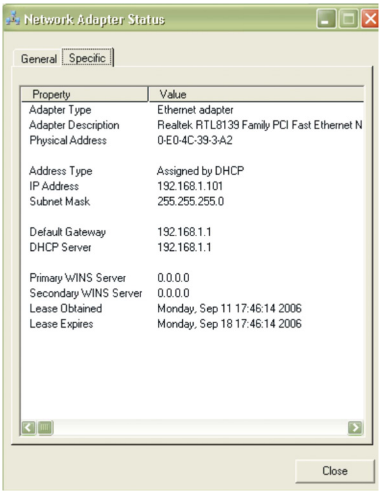
The network adapter status form shown in figure 7 below retrieves the status information of all the network adapters found in the PC.



IP Address: 66.151.2.100

Host Name: bneu-b100.realtimecomm.net

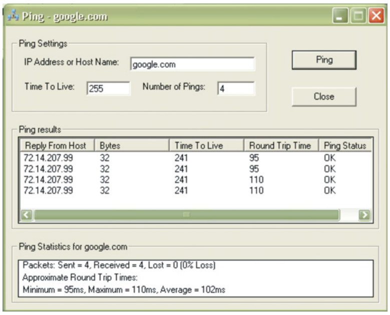
Figure 6: The domain name lookup form



Property	Value
Adapter Type	Ethernet adapter
Adapter Description	Realtek RTL8139 Family PCI Fast Ethernet N
Physical Address	0-E0-4C-39-3-A2
Address Type	Assigned by DHCP
IP Address	192.168.1.101
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	192.168.1.1
Primary WINS Server	0.0.0.0
Secondary WINS Server	0.0.0.0
Lease Obtained	Monday, Sep 11 17:46:14 2006
Lease Expires	Monday, Sep 18 17:46:14 2006

Figure 7: The network adapter status form

The ping form tests for connectivity between a source host and a destination host. Figure 8 is the form used to ping a local or remote host. The form shown in figure 9 is used for tracing the path a packet takes from source host to destination host.



Ping Settings

IP Address or Host Name: google.com

Time To Live: 255 Number of Pings: 4

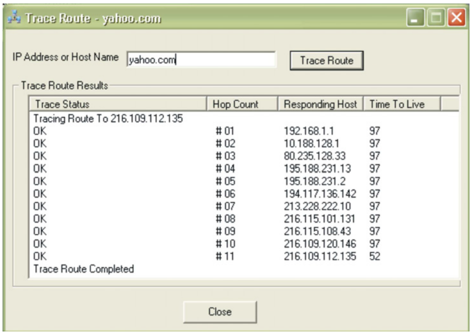
Ping results

Reply From Host	Bytes	Time To Live	Round Trip Time	Ping Status
72.14.207.99	32	241	95	OK
72.14.207.99	32	241	95	OK
72.14.207.99	32	241	110	OK
72.14.207.99	32	241	110	OK

Ping Statistics for google.com

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% Loss)
Approximate Round Trip Times:
Minimum = 95ms, Maximum = 110ms, Average = 102ms
```

Figure 8: The ping form



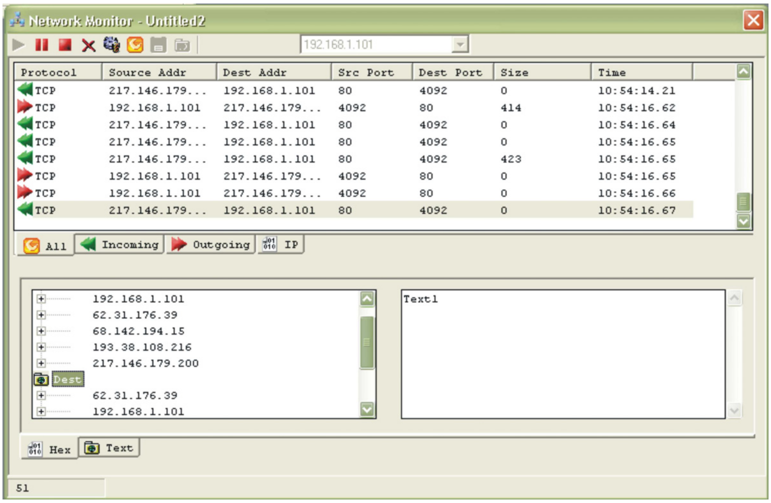
IP Address or Host Name yahoo.com

Trace Route Results

Trace Status	Hop Count	Responding Host	Time To Live
Tracing Route To 216.109.112.135			
OK	# 01	192.168.1.1	97
OK	# 02	10.188.128.1	97
OK	# 03	80.235.128.33	97
OK	# 04	195.188.231.13	97
OK	# 05	195.188.231.2	97
OK	# 06	194.117.136.142	97
OK	# 07	213.228.222.10	97
OK	# 08	216.115.101.131	97
OK	# 09	216.115.108.43	97
OK	# 10	216.109.120.146	97
OK	# 11	216.109.112.135	52
Trace Route Completed			

Figure 9: The trace route form

The form shown in figure 10 is used for monitoring the network in general, based on source and destination IP address, protocols and based on port numbers. The original source of the form was from the Planet Source Code website (http://www.Planet-Source-Code.com/vb/). The general monitoring is based on the network adapter's available IP addresses generated by the code for the form. These addresses can be selected by using the combo box below the form's title bar. The monitoring based on source and destination IP addresses, protocols and port numbers can be done by using filters. The filters can be accessed by using the toolbar below the title bar. The outputs from the form are the inflow of traffic in and out the network adapter and the contents of each packet.



192.168.1.101

Protocol	Source Addr	Dest Addr	Src Port	Dest Port	Size	Time
TCP	217.146.179...	192.168.1.101	80	4092	0	10:54:14.21
TCP	192.168.1.101	217.146.179...	4092	80	414	10:54:16.62
TCP	217.146.179...	192.168.1.101	80	4092	0	10:54:16.64
TCP	217.146.179...	192.168.1.101	80	4092	0	10:54:16.65
TCP	217.146.179...	192.168.1.101	80	4092	423	10:54:16.65
TCP	192.168.1.101	217.146.179...	4092	80	0	10:54:16.65
TCP	192.168.1.101	217.146.179...	4092	80	0	10:54:16.66
TCP	217.146.179...	192.168.1.101	80	4092	0	10:54:16.67

```
192.168.1.101
62.31.176.39
68.142.194.15
193.38.108.216
217.146.179.200
Dest
62.31.176.39
192.168.1.101
```

Text1

51

Figure 10: The network monitor form

3. Research Methods

The aim of this research is to implement a range of network monitoring tools within a single GUI under Microsoft Windows. The functionality of the implementation was specified to include live monitoring of network traffic; monitoring based on IP addresses, MAC addresses, protocols and port numbers; network address look up; domain registry look up; traceroutes and wireless network monitoring. The research methods used in conducting this research include interviews with systems and network administrators to determine the extra features required for inclusion as a tool; review of existing tools and software to identify what is to be improved upon; experimental design for the actual implementation of the network monitoring tools and finally, a survey by using questionnaire to evaluate the tools implemented.

4. User Evaluation

As part of the research method, a survey was carried out using a questionnaire to evaluate the performance of the network monitoring tools implemented. This was done after the testing of the tools. The tools were sent to twenty five targeted users; only 17 participated in the survey by testing the tools and filling in the questionnaire. The analysis carried out on the results from the questionnaire showed that:

Of the 17 respondents:
59% strongly agreed and 41% agreed that the software was simple to use. 71% strongly agreed and 29% agreed that the software was user-friendly. 12% strongly agreed and 88% agreed that the software made good use of a graphic interface. 53% strongly agreed, 35% agreed, 6% do not know and 6% disagreed that the software had no adverse effect on the system while it was running. 65% had no error, 29% had between 1 to 5 errors and 6% had between 6-10 errors. 18% strongly agreed, 76% agreed and 6% do not know that the software recovered from the error(s). 18% strongly agreed and 82% agreed that the software satisfied its aim. 12% strongly agreed and 88% agreed that the software satisfied the objective of having the capability to monitor live network traffic. 35% agreed, 29.5% do not know, 29.5% disagreed and 6% strongly disagreed that the software satisfied the objective of having the capability to monitor a network based on Internet Protocol (IP)/Media Access Control (MAC) addresses, protocols and port numbers. 65% strongly agreed and 35% agreed that the software satisfied the objective of having the capability to perform network address and domain name lookups. 88% strongly agreed, 6% agreed and 6% do not know that the software satisfied the objective of having the capability to determine the connectivity of two network devices. 65% strongly agreed and 35% agreed that the software satisfied the objective of having the capability of finding the routes taken by a packet from source to destination devices. 35% agreed and 65% do not know that the software satisfied the objective of having the capability to monitor a wireless network.

5. Conclusion

Network monitoring tools play a vital role in every network and it is a must have if an organisation is to achieve its ROI. The benefits inherent in using network monitoring tools cannot be over emphasised. It provides that valuable network monitoring information needed for the management of any network. It enhances network stability, reliability, performance and allows for the controlling of the complexities in modern day networks.

Analysis of the survey on the evaluation of the network monitoring tools implemented showed that the research achieved its objectives to an appreciable level.

It is believe that this research will go a long way in creating that awareness on the need for constant monitoring of the network.

6. References

Burke, J. R. (2004) *Network Management: concepts and practice, a hands-on approach*, Prentice Hall, New Jersey, ISBN: 0-13-032950-9

Cheswick, W. R. and Bellovin, S. M. (1994) *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, Reading, ISBN: 0-201-63357-4

ComLab Website (2006) 'Tools for modeling the user-traffic' [Online], Available: http://www.comlab.uni-rostock.de/research/tools.html [Accessed August 2006]

Gaglio, S., Gatani, L., Lo Re, G. and Urso, A. (2006) 'A Logical Architecture for Active Network management' *Journal of Network and Systems Management*, vol. 14, No. 1, pp127-146

Held, G. (2000) *Managing TCP/IP Networks: Techniques, tools and security considerations*, Wiley, Chichester, ISBN: 0-471-80003-1

IEPM Website (1999) 'Monitoring with tcpdump' [Online], Available: http://www-iepm.slac.stanford.edu/monitoring/passive/tcpdump.html [Accessed August 2006]

Leinward, A. and Fang, K. (1993) *Network Management: a practical perspective,* Addison-Wesley, Reading, Mass, ISBN: 0-201-52771-5

Liska, A. (2003) *The Practice of Network Security: Deployment Strategies for Production environments*, Prentice Hall, New Jersey, ISBN: 0-13-046223-3

Miller, M. A. (1999) *Managing Internetworks with SNMP*, M & T Books, Foster City, ISBN: 0-7645-7518-X

Subramanian, M. (2000) *Network Management: principles and practice,* Addison-Wesley, Reading, Mass, ISBN: 0-201-35742-9

WildPackets Web Site (2006) 'WildPackets- Etherpeek' [Online], Available: http://www.wildpackets.com/products/etherpeek/overview [Accessed August 2006]

Windump Website (2006) 'Windump: tcpdump for Windows' [Online], Available: http://www.winpcap.org/windump/ [Accessed August 2006]

Wisniewski, S. (*2003) Advanced Network Administration*, Prentice Hall, New Jersey, ISBN: 0-13-097048-4