Implementing a Visual Network Management Console

O.C.Agbai and P.S.Dowland

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

Abstract

Network management is implemented using a variety of tools. It delivers an automated method of managing network devices and resources. It controls the performance and availability of network services. The aim of this research is to demonstrate that a set of network monitoring tools can be used to show the geographical location of a network problem. It was conducted using the network monitoring tools PolyMon and NetMaCon. PolyMon uses its monitors to monitor different parameters of management information. It generates an alert when a specified threshold is reached and stores the data in the database. NetMaCon uses the stored data to generate a visual display of the location of the network problem.

Keywords

Network monitoring, alerts, notification, network management, trend analysis, PolyMon, NetMaCon

1 Introduction

The potential impact of this research is that it will aid in stabilizing the performance of networks ensuring network availability to users. It will provide an appropriate method of response to network problems. This can be made possible by using a range of network monitoring tools.

The tools used are PolyMon Network Monitor and NetMaCon. A combination of these two tools will be used to monitor a network, generate alerts and respond to the alerts by showing the location of the faulty device on the network. The PolyMon network monitor monitors devices and generates alerts when the monitors fail. These alerts are stored in the PolyMon database. NetMaCon on the other hand interacts with the database to show the visual and geographical location of network problems.

The aim of this research is to implement appropriate network monitoring tools that will display the network problems visually. These tools can be implemented from a single management location on the network. The network monitoring tools should be able to:

- Keep the network alive. Keep-alive tests the connectivity between network components.
- Identify network problems.

- Generate alerts and respond to alerts.

The next section explains the concept of network monitoring and network management followed by an analysis of some network monitoring tool. Section 3 explains the research methodology used. The functionalities of the monitoring tools PolyMon and NetMaCon are described in section 4 while the implementation process is explained in section 5. Section 6 is the conclusion.

2 Network Monitoring and Network Management

Network monitoring is a part of network management that involves accessing and gathering information about networked components (computers, routers and other peripherals) that are being monitored. It also involves generation of alerts when an abnormality is encountered. Network Management on the other hand involves accessing and gathering information, generating alerts and responding to the alert. The response can be either by executing code, shutting down the workstations, rebooting workstations or visual display.

Network monitoring is an automated approach to network management and it consists of three major design areas as suggested by Chiu and Sudama (1992): access to monitored information, design of monitored mechanisms and application of monitored information. In other words, the monitored information needs to be available, a technique for retrieving it should be devised and finally this monitored information should be utilized.

The network information on the system can be accessed in two ways: (Shin et al, 2007) the first is the centralised approach and the other one is the distributed approach. In the centralised approach, the entire network is managed from a single location. This location can be referred to as the management station. A central control is established from here to manage and maintain control over the network configuration, balance and optimise the network resources (Stallings, 1999). The distributed approach involves management from different departmental locations on the network. The control is no longer centralised but distributed across different management stations.

2.1 Network Monitoring Tools

A Network Monitoring Tool examines the functionality of a network and generates alerts when a problem occurs. Network monitoring tools can be classified according to their functionality. Some monitoring tools are designed to monitor based on the performance of the system while others monitor the security of the network, the configuration or the fault. Thus, the choice of network monitoring software solely depends on the reasons for monitoring. The tools can be grouped into:

- Application & Host Based Monitoring Tools
- Flow Monitoring Tools

- Packet Capturing Tools
- Bandwidth Analysis Tools
- Wireless Network Monitoring Tools
- Integrated SNMP Platform Tools

(Moceri, 2006; Keshav, 2006)

2.2 Analysis of Existing Network Monitoring Tools

There are numerous network monitoring tools available with varying features and functionalities. Their unique features however render them inflexible to satisfy the various aims of network monitoring. For instance, a packet capturing tool may not be able to generate alerts. A few monitoring tools are discussed briefly in order to establish their uniqueness, various functionalities and limitations.

PIKT

Problem **I**nformant/**K**iller **T**ool is an open-source Unix/Linux based network monitoring and configuration tool. It is used to manage networks and to configure systems security. PIKT has the ability to report faults and fix them, by killing idle user sessions and monitoring user activities. It uses command line and not a GUI (Graphical User Interface).

FLAME

Flexible **L**ight-weighted **A**ctive **M**easurement **E**nvironment is a Linux based network monitoring tool used for performance and security. FLAME is flexible in the sense that it is possible for users to inject codes that handle packets and get the information that is needed.

SysUpTime

SysUpTime checks for failure and it has automated monitoring capabilities which supports network performance and availability. Failure detection triggers an alert signal either by running a script, sound, email, rebooting, restarting, executing Windows commands, or by posting a web site. It displays graphically and has a map editing function which allows the administrator to add or remove components from the network.

In summary, PIKT and FLAME are both Linux based tools while FLAME is a commercial product. PIKT uses a command line execution which is not graphically interactive but it is capable of reporting faults. SysUpTime on the other hand works on Windows and Linux but it is however not freely available. It is capable of generating notifications and responding to them. It also has a graphical user interface.

The next section will explain the research methods used to discover and develop the tools used in this implementation.

3 Methodology

3.1 Investigation

This research began with investigation to find academic information and documents related to the network monitoring and network management. It was important to find out how network monitoring can be implemented from a single location. This led to further investigation to discover management or monitoring tools.

The next stage of the investigation involved finding the appropriate network monitoring tool to implement. The features of this tool should be able to assist in achieving the objectives of this research. Numerous monitoring tools were discovered in the process as well as the discovery of PolyMon network monitor.

3.2 Software Development and Rapid Application Development (RAD)

The decision to develop a software was considered in order to support the functions of the network monitoring tool PolyMon. This software is intended to be used to give a graphical representation of the networked components. It should make it easier for the network administrator to access information about the network while being monitored in real-time.

Rapid Application Development is a development process that is used to generate software quickly. It adjusts the System Development Life Cycle (SDLC) and reduces development time by using recommended tools and techniques to speed up the analysis, design and implementation steps. Visual Basic 6 programming language can be used to achieve RAD and thus, was used for developing the software NetMaCon.

4 The monitoring software: PolyMon and NetMaCon

PolyMon is an open-source Windows based network monitoring tool. It has three (3) main components: SQL Server Database or the PolyMon Database, PolyMon Executive and PolyMon Manager. The PolyMon Database stores information about the *monitors* and monitored stations. The PolyMon Executive operates in the background by running the *monitors* periodically and storing the results in the database. The PolyMon Manager on the other hand is the Windows-based GUI interface where the settings are organised. The monitors are also defined from this interface. The *monitors* in PolyMon refer to the plug-ins that the software uses in monitoring. For example: the Ping Monitor and TCP Port Monitor.

NetMaCon is a visual basic application which communicates with the information stored in the PolyMon Database to present the visual and geographical location of the monitored network and of alert notifications. This alert can be viewed on a Virtual Earth Map when problems occur showing the area where the fault has occurred. NetMaCon uses the Virtual Earth Map to display a 3-dimensional view some buildings in the University of Plymouth. This map is interactive and responds to click events to display a view of the floors in each building. The click events also reveal the internal network of each floor. The networked devices like the computers and the connecting routers are display. This map responds also to the entries retrieved from the database to display a red sign beside the building whose network has been detected to have a problem.

Both monitoring tools used for this research were chosen because they: work on the Windows Operating System, are freely available (Open – Source Software & developed), have an interactive Graphical User Interface (GUI), monitor in Real-Time and generate alerts and alert responses. Real-time monitoring is the ability to monitor network traffic at the exact time the network traffic is being transmitted. This feature is very important when monitoring a network for network administrators to receive the exact traffic being monitored at the time. It will enable the quick analysis of traffic and rapid responses to faults. The Windows Operating system was chosen against the Linux operating system because Windows being a Microsoft product is the largest operating system used worldwide and is more compatible with other software. Microsoft provides security patches for their products more than any other operating system, therefore, it is considered to be a more secure operating system to use.

PolyMon network monitor was chosen because of its ability to log all information and setting of its monitors in the database. NetMaCon serves as a medium that extracts this information from the database and presents them visually. Due to the lack of funding and resources the open-source tool PolyMon has been chosen coupled with the developing software NetMaCon which also costs nothing to implement. How both tools work together is explained in the Implementation stage.

5 Implementation of PolyMon and NetMaCon

5.1 Structure of this Centralised Management System:

This section will be used to show how the tools PolyMon and NetMaCon will be used to achieve the objectives of this research. The figure 1 below is being used to illustrate the network used for this implementation. The devices being used are two computers named COMPT 1 and COMPT 2 and a router named GATEWAY.

The network management station: is a station on network from which the management activities are performed. In this implementation, the management station is COMPT1 and it comprises of a *manager* (that is the PolyMon Executive) and *Management Information Base (MIB)* or Database (that is PolyMon Database).

The managed device on the other hand is the device which is being monitored by the management station. These devices include hosts and routers. In this case, the managed devices are COMPT 2 and GATEWAY. In conventional Network Management Systems, a managed station will usually have an agent and a MIB, but in this case, because of the nature of the monitoring tool PolyMon, the managed devices are agent-less, thus, they do not have agents and MIBs. Rather, the management station gathers and stores the management information. This information is obtained by the *manager* in the management station by “polling” the managed devices. Polling is a request-response interaction between a managed device and the management station (Stallings, 1999).

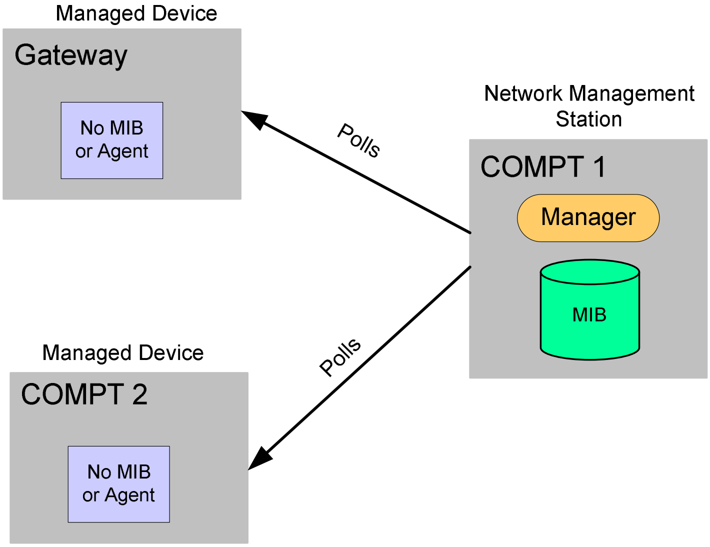


Figure 1: The Management System

PolyMon accesses the monitored information from the managed device using its Monitors. The Monitors controlled by the PolyMon Executive are design to make poll requests from the monitored stations. The poll requests retrieve monitored information from the monitored devices and stores them in the PolyMon database. The monitored information that generates problem notifications is used by NetMaCon to show visually where and when a problem has occurred.

5.2 Implementation Steps:

For the implementation the following are the required hardware and software.

- Processor: 133-MHz (recommended 550-MHz)
- Memory: 128MB of RAM
- Hard Disk: More than 2.9 GB
- Display: VGA that supports console redirection; higher resolution monitor
- Software:

- Microsoft Windows XP operating system (or Windows Server 2000/2003)
- Microsoft .NET Framework 2.0
- Microsoft SQL Server 2000 Developer Edition

The first step is to open NetMaCon and run PolyMon to define the PolyMon Monitors. PolyMon can be opened from within NetMaCon (see Figure 2). This implementation will use PolyMon's Ping Monitor to illustrate how the system works. The Ping Monitor works just like the command line tool *ping*. It sends ICMP (Internet Control Message Protocol) echo requests to the devices on the network. The managed devices should respond to this by sending an echo reply. This confirms the connectivity of the network devices. The Ping Monitor is configured for each device on the network (COMPT2 and GATEWAY). After the configuration, the status of the monitor is tested. This is to confirm that the monitor works properly. The test will return either an **OK** or a **FAIL** indication. The information about the configured monitors is stored in the database. As the PolyMon Executive run these monitors, and OK is stored against the monitor when it works well while a FAIL is stored when the monitor fails. In this example it will mean that the device did not respond to the Ping request.

The PolyMon interface is minimised but it continues to run in background. From the NetMaCon Window, the **Start Reporting** button (see figure 2) triggers the connection to the PolyMon Database. As the PolyMon Ping monitors run, NetMaCon checks the status of the monitors. When FAIL is detected from the database, the background of the affected device changes to RED. This signifies that the device has failed to respond. The device's background turns green when the monitor status is OK.

NetMaCon will show a red alert on the Map against the building whose network has been affected to notify the administrator visually. This signal is shown when NetMaCon receives twenty (20) consecutive FAIL records from the database. Figure 2 gives an illustration of how the alert is being displayed. It shows a red sign near the Babbage building on the map, one on the affect floor labelled "Fault!!!" and then on the background of the two computers on the network. The red alert on the Map directs the administrator to the source of the problem.

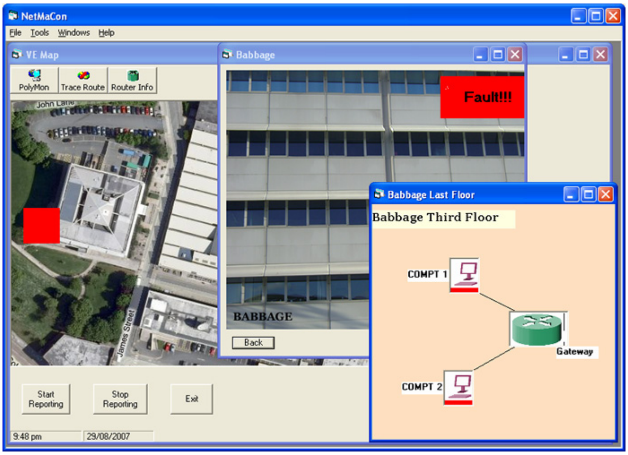
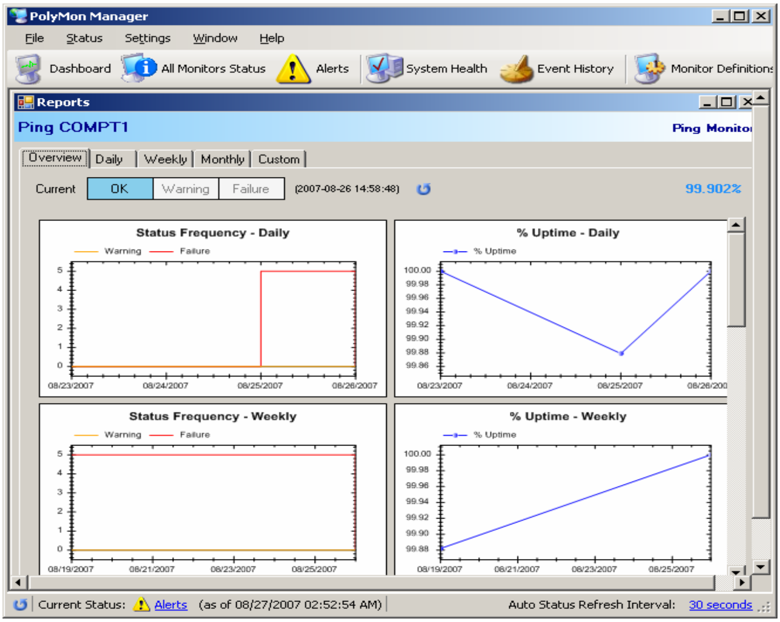


Figure 2: NetMaCon Interface

5.3 Trend Analysis

PolyMon is capable of providing historical trend analysis based on the activities of the monitors. The statistics can be used in the future to prevent the reoccurrence of such faults and failures. Figure 3 below shows the historical analysis of the Ping Monitor for COMPT 1.



Current Status: Alerts (as of 08/27/2007 02:52:54 AM)

Figure 3: Historical Analysis of Ping Monitor for COMPT 1

The figure shows an overview of the frequency of the monitor's daily and weekly status. The daily status shows that the monitor failed between 23rd and 25th of August. From the 25th, there is a rise in the performance of the monitor. The weekly summary shows that the monitor has been working the whole week from the 8th to the 25th of August. The daily percentage uptime shows that the monitor's highest points were the 23rd and 26th of August with 100% uptime, while the lowest point was on the 25th with percentage of 99.88%. The weekly summary shows a continuous rise in the uptime of the monitor. Such information can be used for future references about the performance of the device.

6 Conclusion

6.1 Evaluation

The implementation above demonstrates how PolyMon and NetMaCon attempt to help achieve the objectives of this research. It has been used to keep the network alive using the Ping Monitor which tests the connectivity of network devices. Thus, the tools can be used to effectively identify network problems. However, they have some inadequacies. Firstly, these tools cannot populate the network devices by themselves. Thus, installing new devices to the network will mean manually changing the static networks presented. Secondly, each monitor in PolyMon needs to be configured for individual devices. The configuration stage can therefore be a tedious task.

It is recommended that in future research, a tool that populates the network devices is used to complement the ability of visually displaying notification alerts. This will enhance the functionality of the system. In addition, the visual display of the actual network can also be enhanced when this feature is incorporated. In 3D, the physical location of a faulty network device can be discovered.

6.2 Summary

In summary, network monitoring is a part of network management that uses network monitoring tools to gather information about networked components. Implementing monitoring tools can be done from a single centralized location on the network. The type of monitoring tool used depends on the reasons for monitoring the network. The Windows-based tools used for this implementation are PolyMon and NetMaCon. The conjunction of both tools has provided an effective interactive GUI tool that monitors the network for problems and generates visual notifications. The tools are used effectively to report alerts generated when faults occur on a network and can be used to predict device failures.

7 References

Chiu, D. M. and Sudama, R. (1992) *Network Monitoring Explained: design & application,* Ellis Horwood Limited, England, ISBN: 0-13614-710-0.

Keshav, T. (2006) *A Survey of Network Performance Monitoring Tools* [Online], Available: http://www.cs.wustl.edu/~jain/cse567-06/net_perf_monitors1.htm (21/01/07)

Moceri, P. (2006) *SNMP and Beyond: A Survey of Network Performance Monitoring Tools*, http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors2.pdf (15/01/07).

Shin, K. S., Jung, J. H., Cheon, J. Y. and Choi, S. B. (2007) 'Journal of Network and Computer Applications' *Real-time network monitoring scheme based on SNMP for dynamic information*, 30 (1): pp 331-353.

Stallings W. (1999) *SNMP, SNMPV2, SNMPV3, and RMON 1 and 2,* Addison Wesley Longman: Massachusetts, ISBN: 0-20148-534-6.