# The Art of Network Monitoring

A.Mohyuddin and P.S.Dowland

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

## Abstract

This research paper focuses on different types of Network Monitoring techniques and putting micro level details on various elements that contribute to a good network monitoring platform. There are thousand of network monitoring systems available in the market; it is hard to conclude which system is best to requirements and what elements needs consideration when making a choice, some good monitoring systems has been discussed in this research paper.

## Keywords

Network Monitoring, Network Monitoring Tools

## 1. Introduction

Network monitoring systems can be seen as a complete solution to constantly monitor the network performance against any failures, bottlenecks or unusual activities that can result in slowdowns or breakdowns of computer networks. Today network monitoring systems are working along with security applications to prevent computer network from outside world and any vulnerability within the organization. A recent study conducted by computer security institute (Flukenetworks.com, n.d.) and FBI revealed that out of 264 companies surveyed 53% of the companies detected un-authorized usage of the company's network and approximately 50% of un-authorized usage was reported within the organization. These figures are very alarming as companies now just do not have to secure themselves from the outside world but also within the organization.


**Figure 1: Problem solving with network monitoring (Network Probe, 2006)**

Modern network monitoring systems are more responsive then they were ever before, they analyze network usage and study different behavior on the network at all the times and solve problems which they can or have ability to alert it to network administrator immediately incase of any security breach. It is also important to understand that intruders have access to complicated technology, so if any company or an organization wants there networks up and running they have to be secure in a better way; it is also important to point out that company employees always find a

way to breach security policies, any malicious software being installed by any employee can leak out company's data to outside world.

## 2. Types of Network Monitoring

### 2.1 Passive Network Monitoring

Passive network (Ciuffoletti, 2006)Monitoring technique examine network traffic by scanning individual packet, this process allows to study patterns on network and helps to determine packet flows. The advantage of using passive network monitoring is that there is no need to insert additional packets, hence keeps the traffic on the network low.

Passive network monitoring (Timm, 2003) is helpful when network administrator need to know very low level detail about the network such as network topology, services, operating system, and application being used at different nodes. This is achieved by scanning TCP and IP headers using various packet sniffers such as Tcpdump or an Ethreal. A variety of information can be gathered just by analyzing a packet such as host logical location can be determined by just determining the TTL field of the IP header. Filters can be created to gather information from the packets and this information can help to determine if there are any vulnerabilities to the network.

### 2.2 Active Network Monitoring

Active network monitoring works by injecting packets into the network or send it to workstations, servers, applications etc to measure network performance. The problem lies in sending extra packets which sometimes create an extra traffic, but usually little amount of packets can be used to attain desired information. In addition active network monitoring allows a full control over additional packets that are required to be sent over the network, these can be sent whenever required by any specific monitoring application hence are more flexible.

### 2.3 Hybrid Network Monitoring

Hybrid Network Monitoring (Landfeldt, 2000) is an emerging technique to monitor large number of growing wireless Networks, As the name suggest Hybrid network monitoring make use of active monitoring where passive network data is unavailable and vice versa. The passive monitoring on a wireless network can only be used in case of an open connection; if there is no open connection active monitoring techniques will be used. Imagine two segments of a wireless network; which are wired and wireless.

## 3. Core of Network Monitoring

Network monitoring covers an extensive range of features; its dimension goes from monitoring different operating systems to checking memory usage or downtimes of devices attached to the network and there are many more potential features offered

by good monitoring packages. There are different types of network monitoring which are as following:

### 3.1 Bandwidth and Traffic Monitoring

Bandwidth and traffic monitoring helps network administrators to determine any vulnerabilities to the network. Traffic and bandwidth monitoring allows:

- Avoiding any bottlenecks on networks
- Worms entering into the network can be tracked down by looking at the traffic trends
- Nodes with high data transfer rates can be determined for any further investigation
- Bandwidth monitoring can make it easier to avoid any extra cost or quality constraints

Bandwidth and Traffic (Paessler.com, n.d.) monitoring works by recording all outgoing and incoming packets and maintaining a record of how many packets has been transferred and how many packets has been received. Usually traffic monitor maintains its own database for this purpose, however traffic and bandwidth monitor make use of standard protocols such as SNMP, Net flow and various packet sniffer record network usage.

### 3.2 Performance Monitoring

Performance monitoring collects data at various points from where the traffic is being passed; it monitors the packets flow, packets being successfully transferred and packet loss, availability, CPU load, memory and disk space utilization. This would allow network administrator to look for any slow node or any point where network performance is not up to mark. Network performance monitor software can interface with SNMP and supply information about nodes that are on network.

### 3.3 Security Monitoring

Network security monitoring (Ferraro, 2003) works closely with Intrusion detection system (IDS) and collects event logs, session logs and historical data and identifies any intrusion. Network security monitoring is usually event driven, and alerts when any event occurs to breach security,

### 3.4 Application Monitoring

Application monitoring can help network administrators to solve any problems well before time by looking at each application behavior, and how application is performing technically. Application monitoring can help to distinguish nature of the problem caused by applications on the network, can help to restart the application if they are causing any problems. Application monitoring (Polozoff, 2003) works by analyzing large amount of system and event logs and its frequency of occurrences;

this enables to analyze problems at very earlier stage before things start getting to worst.

### 3.5 Packet Capturing and Protocol Analyzer

Packet capturing and (Packet sniffer, n.d.) protocol analyzers are the software or hardware that has ability to intercept the traffic that is passing through a particular network point, this enables to study network behavior including any problems solving, knowing more about network, network usage etc. Capturing packet allows working on many more application of network monitoring, there are various implementation being used by various applications to transfer packets (approved by RFC) which can help to analyze what applications client are using but it is however considered as less secure and data integrity is damaged by any such of the monitoring device or software.

### 3.6 Database Monitoring

Database monitoring (Monitoring, n.d.) works by observing a database application on the server, functionality includes querying database after regular interval to see the query response time, disk space, database availability, database access, usage, data creation change or deletion etc, since a database is really critical to business database monitoring also monitors the server machine by checking machine performance, CPU usage, or by studying background processes.

### 3.7 Web and Email Server Monitoring

Web site monitoring includes accessing a web page (Network Monitoring Tools, n.d.) and domain name servers (DNS) resolution after specific interval of time. A query is made to resolve an internet address, incase of a no response administrator are alerted. Email server use SMTP to send and receive emails, mail server monitoring includes SMTP handshaking with specified mail server by sending an email and receiving an automated response. In case if there is a no response of handshake network administrators are alerted about the problem.

Third party web and email monitoring solutions make use of various check points around the globe and they use various methods to ensure that your network is accessible around the world by testing it from various places.

## 4. Reviewing network monitoring tools

There are thousand of network monitoring tools available in the market equipped with latest features and technologies that allows network administrators to take control over network even from remote location. Good network monitoring systems are capable of monitoring large number of different devices, compatible with various platforms, analyze network resources and filter very micro level network details but what really makes them a good choice is features that gives network administrator a facility to get indication before worse happen. This is usually achieved by analytical engine present in network monitoring systems. There are many issues to consider

when choosing a network monitoring system such as level of detail being analyzed for resource discovery, alert time, number of devices being supported by and number of networks that can be monitored over a large geographical area; some of the good networks monitoring systems equipped with such technologies are discussed below:

ManageEngine OpManager is one of the complete networks monitoring system; it monitors a very micro level detail of the network devices over a large geographical area. Backed by a good customer service this system cost really high and any organization with critical network can afford to keep it running. There are some freely available network monitoring tools available such as Nagios and Kismet; these systems are capable of reporting network faults via email and text messages and available as an open source free to implement and distribute under public license. The only problem lie is lack of customer support and hard implementation process, expertise are required to implement these monitoring system and look after.

## 5. Conclusion

Network monitoring tools are key elements for survival of any computer network, although there are lots of network monitoring tools available but there is a further research available on various methods such as Hybrid network monitoring. Also Hybrid network monitoring is gaining momentum as the new generation of networks is a combination of wired and wireless clients. This particular area needs researcher's attention and new hybrid monitoring platforms are needed to be developed for local and remote networks. It is also important to mention here that the next generation of computer networks will involve VoIP applications thus current network monitoring tools has to expand there functionalities to VoIP applications monitoring.

## 6. References

Ciuffoletti, A. (2006).*Architecture of Network Monitoring Elements*. Retrieved August 1, 2006, from web site: www.coregrid.net/mambo/images/stories/TechnicalReports/tr-0033.pdf

Cottrell, L. (2001). *Passive vs. Active Monitoring*. Retrieved August 1, 2006, from web site: http://www.slac.stanford.edu/comp/net/wan-mon/passive-vs-active.html

Ferraro, C. (2003). *Network security monitoring*. Retrieved August 1, 2006, from web site: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci922007,00.html

Flukenetworks.com (n.d.). *The cost of network security failure*. Retrieved August 1, 2006, from web site: http://www.flukenetworks.com/fnet/en-us/findit?Document=2422673

Landfeldt, B. (2000). *The case for a Hybrid Passive/Active network monitoring scheme in wireless internet*. Retrieved August 1, 2006, from web site: http://www.cs.usyd.edu.au/~bjornl/research/papers/icon2000_landfeldt.pdf

Monitoring. (n.d.) Retrieved August 1, 2006, from web site: http://database.ittoolbox.com/topics/t.asp?t=331&p=343&h1=331&h2=343

Network Monitoring Tools. (n.d.) Retrieved August 1, 2006, from web site: http://www.dotcom-monitor.com/network-monitoring.asp

Network Probe. (n.d.) Retrieved August 1, 2006, from web site: http://www.objectplanet.com/probe/

Packet sniffer. (n.d.) Retrieved August 1, 2006, from web site: http://en.wikipedia.org/wiki/Packet_sniffer

Paessler.com. (n.d.). *Bandwidth and Network Usage Monitoring Made Easy*. Retrieved August 1, 2006, from web site: http://www.paessler.com/prtg

Polozoff, A. (2003). *Proactive Application Monitoring*. Retrieved August 1, 2006, from web site: http://www.ibm.com/developerworks/websphere/library/techarticles/0304_polozoff/polozoff.html

Remote Monitoring. (2002). Retrieved August 1, 2006, from web site: http://searchmobilecomputing.techtarget.com/sDefinition/0,290660,sid40_gci214268,00.html

RMON. (n.d.) Retrieved August 1, 2006, from web site: http://searchmobilecomputing.techtarget.com/sDefinition/0,290660,sid40_gci214268,00.html

TCP/IP Remote Network Monitoring. (2005) Retrieved August 1, 2006, from web site: http://www.tcpipguide.com/free/t_TCPIPRemoteNetworkMonitoringRMON.htm

Timm, K. (2003). *Passive Network Traffic Analysis*. Retrieved August 1, 2006, from web site: http://www.securityfocus.com/infocus/1696