

## Network Management and Monitoring Software

Many products on the market today provide analytical information to those who are responsible for the management of networked systems or what the users of those systems commonly call "The Network". The discussion below clarifies the general use of the terms *Management* and *Monitoring*, outlines the broad product categories, discusses the costs of poor system performance and describes the specific monitoring functionality of network management software.

### Monitoring and Management

Many of these product types tend to be described as *Network Monitors*, which is a very generic description. *Monitoring* is one of those terms that can get confusing as many products are positioned under this broad category. And, without a doubt these products monitor, although they may have very specific functionality. It is important to get past the Network Monitor terminology and understand what a product really monitors or analyzes.

The *Management* aspect of these products comes from statistical reporting and event notification that is triggered by the monitoring. This is sometimes referred to as fault management. Statistical reports can be generated from continuous data collection to baseline the network, client and server. This reporting can be used to be proactive in providing adequate resource for the monitored system. Event notification alerts administrative users to high or low thresholds above a baseline or the existence of adverse conditions.

Hardware components need to be configured and software agents will need to be installed. The sophistication of the agents and the placement can require detailed knowledge of client, server and network architecture. For example, understanding application and user utilization of network bandwidth requires tapping into the wire and capturing packets at strategic points on the network.

### Broad Product Categories

No one tool will satisfy all needs. The reason is fairly straight forward, as functionality dictates the architecture. Tools needed for troubleshooting may require passive architectures, where reporting and monitoring can be quite active. Some products can sample information and others may need to capture all of the data. Other features that include expert analysis for troubleshooting or security may require different development skills than those needed for server monitoring. Also, the user console design is dependent on the functionality.

The categories described are general in nature and can have crossover functionality in a number of products.

**Some Examples:**

- Enterprise Management - Complete solutions for the enterprise, with integrated network & system management, database management, application management. Service Level Management is also a component that measures actual quality of service to agreed targets. It is not unusual for these products to be comprised of modules and be very encompassing including features such as Job Scheduling. Many older Enterprise products can be very complicated to use and configure. Newer products with more modern architecture will still require days to configure.
- Network and System Monitoring - Enhanced commercial network & system monitoring tools. This user might be a NOC (Network Operations Center) wanting to manage Network and Servers. The functionality can be very similar to the Enterprise management.
- Network Traffic Analysis & Performance Monitoring - Traffic flows through and between critical network devices, utilization statistics; performance monitoring of network traffic.
- Application Monitoring - monitor application behavior and performance. Is it the application, network, client or server? It also can get very specific focusing on specific databases or e-mail systems.
- Device Monitoring - Record and view activities of Servers and Devices in a network environment. Can be as simple as up or down.
- Security Monitoring - Security monitoring of network, workstations and servers. Generally any product that is used to protect or audit threats.
- Web Monitoring - Web monitoring and web analyzing tools.
- Protocol Analyzers and Packet Capture Tools - Packet capture tools, network sniffers and packet monitors.

All these tools have the same objective – keep systems operating efficiently and if not, get to the root cause of the problem and resolve the problem so systems run efficiently.

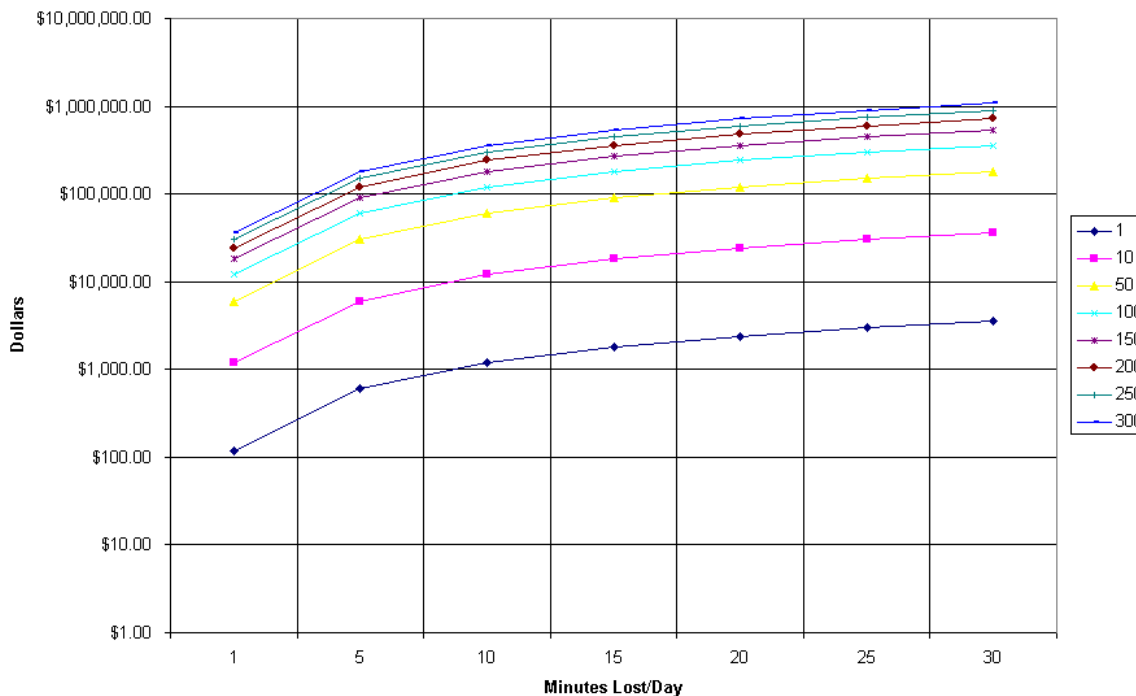
## Cost of Poor System Performance

Ever call a company for information only to be told they can't help you because the system is slow or down. What is the cost?

Without tools those responsible for these systems need to use very labor-intensive methods to root out problems. In some cases without some sort of tool the root cause of the problem would be impossible to discover. The proper tools can provide a substantial reduction in costs. The following graph illustrates just one of the costs, user down time or response time. But there can be many costs when performance issues arise, such as lost or unhappy customers that translate into lost sales or the lost time Network Engineers spend to resolve problems.

**Network Down Time and Response Time issues can have a significant cost impact on the User community.**

Annual Performance Cost at \$20 per Hour by Number of Impacted Users



As shown above network management tools can very quickly be justified take alone the cost impact on the user community. For example from the graph above 10 users losing on average ten minutes per day from either system down time or from performance problems has a cost impact of over \$10,000 per year and where 300 users can be over \$500,000. This demonstrates that this is an issue for both large and small businesses.

## Monitoring Categories

Depending on the business needs, different tools need to be deployed to prevent costly downtime or slow performance. Broken down below are some of the more specific functional categories of Network Management Software products.

## SNMP Device Monitor

Short for ***Simple Network Management Protocol***, a set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages to different parts of a network.

SNMP-compliant devices, called *agents*, store data about themselves in *Management Information Bases (MIBs)* and return this data to the SNMP requesters. Examples of managed devices on a Network include Servers, Switches and Routers.

SNMP Device monitors can take the form of a management station gathering and displaying information from managed agents. A management station is the location where an administrator can view, analyze, and even manage network devices. SNMP traps and alarms can be sent to network and system administrators. This again creates a pro-active environment that reduces the time users are impacted.

In today's switched network environment it provides Network Analysts port statistics that can help narrow in on devices that may be causing problems reducing troubleshooting time. SNMP on server can also relay device CPU usage and other information.

## Device Monitor

Low end products typically monitor only the status of network devices, and many generate a graphical map of your network. This map is typically used as a console interface to select devices to monitor - these are most often Servers and Printers. Basic features actively test connections and ports (Services) or do a trace route to verify active links. When a connection is lost, a notification system can send warnings to a console or notify administrators by pager or email. This creates a pro-active environment that reduces the amount of time users are impacted. These device monitors are more likely to be used by System Administrators.

However, the sophistication of enterprise device monitoring can be very device specific. Users can customize the console interface, alerts, and include defined service levels in their reporting and monitoring.

Enterprise device monitors can obtain information from devices by using a number of methods, most common are SNMP, ICMP or software installed to probe and monitor the device.

## Server Monitoring

These monitors provide information on CPU, Memory and disk space usage; they can also monitor the availability and performance of applications, databases and servers. This category of software tends to be a very advanced and specific form of Device Monitoring.

Enterprise products can include monitoring processes, services, print queues, network interfaces, directory and file systems.

## Network Application Monitoring

This type of software can help Network and System Administrators understand how the applications flow through the WAN/LAN infrastructure. These tools collect detailed performance metrics about network traffic, applications, latency, and response times.

Having a view of applications over just protocols allows the networking staff to clearly and quickly identify and troubleshoot network problems by providing the information necessary to understand the interaction between applications and the network. System Administrators, Network Administrator, Network Engineer and Planners use these tools.

Another type of application monitoring may encompass both server and the specific application or applications running on the server. This can include Database servers, Web servers, Middleware servers and even servers that provide directory services like DNS or DHCP.

### **Database Monitoring**

It becomes importance to monitor the database to provide high availability and peak performance. In addition to monitoring server resources database applications can require monitoring of table size, threads, fragmentation, I/O, buffers and logs.

## **Web Monitoring**

This type of monitoring focuses on web servers and the associated network protocols, ports. They can vary from monitoring conversations to server performance. Conversation monitoring can include source, browser type, hits, sessions, session times and pages viewed.

## **Client Monitoring (Service Levels)**

These more specific device-monitoring tools provide a complete measure of end-user experience by tracking response times, resource usage, application faults and availability. These tools not only verify service levels are being met but also can be used proactively when the service level tends to trend downward.

## **Security Monitoring**

These products provide network security tests, security information, or network security services, and security assessment reports. Many of these are very specialized products. Firewalls, Anti virus, Spam and Spy Ware blocking are one form. Other tools can map and audit devices and notify of rogue or unauthorized devices. Wireless and mobile technology creates security-monitoring issues both in and away from the office.

## **Protocol Analyzer**

These network tools often have built-in intelligence that helps those who manage and troubleshoot the network. Analyzers capture packet information to examine the flow of traffic on the network. They provide an instant picture of the traffic situation by monitoring network traffic in real time, to identify and isolate network traffic problems and congestion. They provide detailed information on what computers are active and the protocols they are using to communicate to other devices.

Expert system features eliminate the need to sort through thousands of packets to discover and quantify error conditions. They also provide advice on ways to correct the problem. Filters can be utilized and alarms set to identify computer viruses and locate the infected device. All good analyzers have notification features.

Analyzers have been evolving as the tool of choice for network forensics, audit and application performance troubleshooting. It is the detail of the information they collect over time that make them ideal for such tasks.

Analyzers come either as Hardware or as Software usually installed on Windows based PC's. They may also have distributed probes to monitor remote network segments locally. Probes are designed to tap into the physical layer of the network such as fiber and wireless.

Good software analyzers should be usable by any network administrator, regardless of his or her experience level. Network Administrators and Engineers typically use these tools. These tools help reduce the time spent to resolve network problems reducing cost of down time and increasing the engineers productivity.

## **Application Performance Analyzer**

This special class of Analyzers determines the root cause of poor application performance. Software code, system architecture, server hardware and network configuration can impact an applications performance. These tools provide you with information on how the system as a whole is behaving.

Application Performance tools will break down the client and server's performance, network bandwidth and latency. They provide a map of the conversation where suspect code can be evaluated. The most sophisticated tools in this area have a high level of drill down capabilities and can provide information gathered from both Client and Server or Server-to-Server conversations. Network Administrators as well as Development may use these tools.

## Summary

General tools such as protocol analyzers or mapping and device monitoring software offers a great front line to managing networked systems. They offer affordability for both large and small organizations. Enterprise monitoring products offer substantial depth in a single product and can be customized to an organization's needs. These sophisticated tools typically are feature rich and thus more expensive. Other monitoring tools will be needed to support special needs such as security.

### About the Author:

Bruce Warner is the owner of Operative Software Products [www.operativesoft.com](http://www.operativesoft.com). He has over 20 years experience in the computer field, primarily providing software solutions for managing enterprise systems. Operative Software Products operates in the United States and Canada and markets software that builds, tests, diagnoses and operates the IT infrastructure.

Copyright 2005