Study of Network Performance Monitoring Tools-SNMP

Mr. G.S. Nagaraja, Ranjana R.Chittal, Kamod Kumar

Sr. Lecturer, Dept. of Computer Science & Engg.
R.V.C.E, Bangalore M.Tech,Dept. of C.S.E

Summary
Computer networks have influenced the software industry by providing enormous resources distributed around the globe and interactions among people working anywhere in the world that the world today seems too small. Networks themselves have undergone a radical change in the last few decades starting from ARPANET to the Inter-Continental data cables that we see today. The amount of data that is carried on the Information Super Highway has been increasing everyday prompting for efficient management of the Trans-Continental Super Highway of data. The growing dependence on networks for everyday tasks has created the demand for high performance; reliable networks thereby making companies invest a lot on research on improving the networks and new designs. Part of achieving the goal of high performance is active monitoring of networks to help in the identification and prevention of network errors. Many tools have emerged to aid in performance monitoring of networks. The most common class of tools is based on the Simple Network Management Protocol (SNMP), a protocol for sending and transmitting network performance information on IP networks. Other types of network performance monitoring tools include packet sniffers, flow monitors and application monitors. Examples of the various monitoring tools are SolarWind's Orion SNMP monitoring platform, WireShark packet capture tool, Webmetrics' GlobalWatch and Cisco's NetFlow flow monitoring tools.

Key words:
Simple network management protocol, internet protocol, monitoring tools.

1. Introduction

Data Networks have penetrated in our day-to-day life in a big way, wherein we cannot think of any organization to run without on or the other form of it. Networks have evolved themselves into forms never thought of before with a large demands for tools and technical staff to man them. Companies have invested on their networks in a huge way and they are looking forward to achieve zero downtime for their network. One of the approaches that has gained popularity with this high demand is the concept of network monitoring either Active or Passive to collect data and improve upon the networks. This has lead to the development of numerous network performance monitoring tools and standards. The most common tools are network management system based on standardized network management protocols that give a comprehensive view of a network and all of its devices. Of course, there are other tools that are not as complex as a full network management system but are equally useful for monitoring certain aspects of network performance.

This survey paper will cover the basics of network performance monitoring, standards for network management and different types of monitoring tools. It will conclude with a look at several different monitoring tools including commercial and open-source implementations.

1.1 Terminology

The following definitions are important for understanding the basics of network management and performance monitoring and will be used throughout this survey paper.

(a) **Agent:** A piece of software that acts for the user or other program such that they act on behalf of the user or the program.

(b) **Managed Device:** A device that is capable of participating in a network management system either for collecting statistics or running a program to assist in device management.

(c) **Management Information Base (MIB):** A hierarchical specification of the management data on a managed network device.

(d) **Management Station:** The software that sends requests to agents and receives traps on behalf of an administrator or management software. Also known as the Manager.

(e) **Network-Management System (NMS)** A complete hardware and software system that monitors and manages a network.

(f) **Simple Network Management Protocol (SNMP)**: A network protocol that is part of the Internet Protocol suite used to send and receive network management information.

(g) **Trap**: Asynchronous messages sent by agents to managers. May be used for alerts or event notifications. Also known as Notification.

Manuscript received July 5, 2007
Manuscript revised July 25, 2007

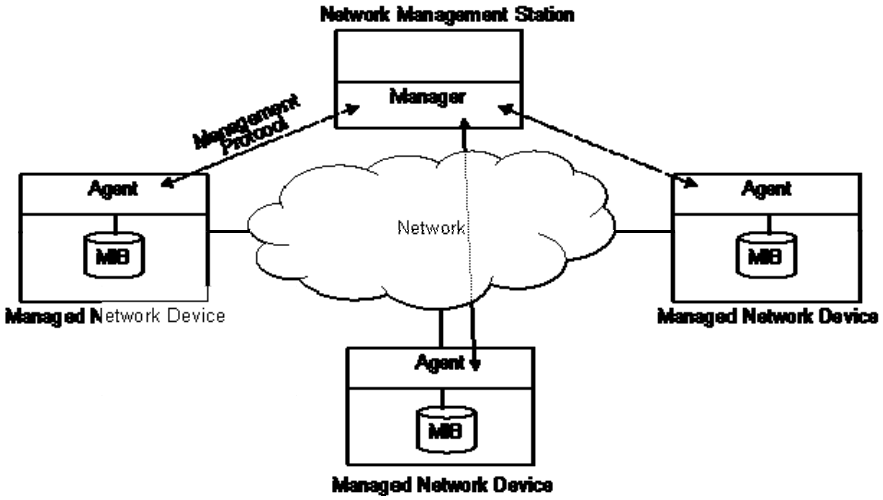

Fig 1. A network management system composed of a management station and several agents.

Table 1. Various performance metrics useful for network administration and engineering.
Metrics are classified as lower is better (LB}, higher is better (HB), or nominal is best (NB) [1]

Metric	Classification	Description
Availability	HB	Measure of what percentage of the time a network resource is available for use. Clearly, high availability is better because down time is not welcome.
Throughput	HB	A measure of how much data can be sent on or through a network resource in a given time period. Also referred to as available bandwidth. Higher throughput is certainly better from users' and administrators' points of view.
Utilization	NB	Measure of the usage of a link, port, or network resources. Nominal is best because high utilization is accompanied by high delays and low utilization is seen as a poor use of resources.
Delay	LB	The amount of time for a packet to traverse, either one-way or round trip, a network, network segment or network device.
Error Rate	LB	Usually refers to the percentage of packets or bits that contain errors on a network link, segment or device. High error rates can signal to an administrator that there is a problem in the network.

1.2 Terminology

The most popular means of monitoring network performance are network management systems. a network management system, as depicted in Figure 1, consists of a centralized network management station and management agents running on network devices. Using a management protocol, the management station polls agents for information about the network devices. Agents return requested information ranging from bandwidth usage to CPU load. Using this information, the network management system provides performance and error reporting to network administrator.

Network management systems are by no means the only form of network monitoring. This survey will cover several other types of network monitoring tools including packet captures tools, flow monitors and application monitors in addition to network management systems. Before covering specific types of monitoring tools, it is important to understand what information monitoring tools provide to network administrators and the metrics they use.

1.3 Terminology

Network performance monitoring tools provide a variety of information to network administrators and engineers through the use of various performance metrics.The most commonly talked about metrics in the networking arena are availability, throughput, bandwidth utilization, and latency (or delay). However, administrators are also often interested in error rates and the performance of network devices including CPU and memory utilization and delay (or latency). Each of these metrics can be classified as lower is better (LB), higher is better (HB) or nominal is best (NB). This classification system is taken from Jain [1]page 40. Table 1 lists the mentioned performance metrics, their classification and a description of why they are useful.

2. Types of Monitoring Tools

2.1 Integrated SNMP Monitoring Platforms

An integrated SNMP Network Management System is one that leverages SNMP to give a complete view of a network. Integrated monitoring platforms actively collect network information from network devices and analyze the data. Most integrated platforms provide graphic reporting, monitoring, and administration of networks allowing easy management and setup of monitoring. Complete monitoring systems provide detailed and comprehensive analysis of network performance. Common performance characteristics include bandwidth utilization, throughput, response time, and error rates as well as CPU load and memory utilization of the network equipment and servers. In addition to real-time monitoring and reporting, SNMP network management systems also provide alerts based on any of the monitored performance characteristics.

2.2 Passive Analysis

Passive network performance tools, also called packet capture tools or packet sniffers, are the class of network tools that do not generate any traffic themselves while collecting data. Instead, the analyzer merely listens to traffic that is on the network. This fundamentally limits the breadth of analysis generated by passive tools because they can only see traffic that is local to the device running the analyzer. For example, in a switched Ethernet environment, a passive system would only see traffic sent to or from its host [2].

2.3 Application and Service Monitoring

Application and service monitoring refers to the class of performance monitoring tools that provide monitoring of individual network applications. Application monitoring depends less on the network equipment and infrastructure and more on the actual servers that provide user services. Such tools provide reporting on application availability, utilization and performance as well as performance characteristics of the underlying server. One common use for application monitoring is website availability monitoring. However, other uses can be built on protocols and services much more complex than HTTP. Database monitoring may consist of transaction rate, server load, memory and disk usage, and concurrent connection count. Administrators can use this information to easily identify and resolve application problems and evaluate infrastructure performance for bottlenecks or excess capacity.

2.4 Flow Monitoring

Instead of looking at traffic from a packet level, flow monitoring analyzes network traffic as flows. Flow monitoring aggregates network traffic based on individual connections, users, protocols, or applications. This allows flow monitoring tools to provide a bigger picture view of a network including specific information on application and connection performance as well as insight into routing and even network security. This view of the network performance aids in network planning as well as traffic engineering because of the traffic trends flow monitoring is able to identify [7].

2.5 Comparison of Performance Monitoring Tool Types

Table 3 summaries the different types of monitoring tools and highlights the differences among them. The majority of the types are active which makes them much more comprehensive. Also, the different systems vary a great deal in which layer or layers of the network stack they operate in.

Table 3 Comparison of different types of network performance monitoring tools.

Type	Passive or Active	Network Layer of Operation	Basic Operation
Integrated SNMP Platform	Active	Data Link and Network	A management station polls agents on network devices to gather information about the network
Packet Capture/Sniffing	Passive	Data Link	Listens for and captures packets on a network device for analysis
Application/Service Monitoring	Active	Application	Actively polls applications and application servers to provide performance information
Flow Monitoring	Active	Transport and Higher	Monitor connections and flows on the network for higher layer trends

3. Example Implementations

There are countless different network performance tools of varying type available today. Commercial products as well as open-source projects provide options for monitoring networks. The intent of this survey is not to be a comprehensive listing of performance monitoring tools but rather to give a glimpse of the variety of tools available. A fairly comprehensive list of different tools can be found in [3].

3.1 Integrated SNMP: SolarWinds' Orion Network Performance Monitor

SolarWinds provides a variety of network management solutions ranging from individual monitoring tools to complete, full-featured monitoring platforms. Orion is their comprehensive monitoring solution built on SNMP. The Orion management application features a web interface with real-time monitoring of availability, bandwidth utilization, network latency and many other network performance metrics. The system automatically summarizes data and prioritizes events and alerts for easy monitoring and troubleshooting. Each event, statistic or alert also has a drill-down feature which provides all of the details on a given piece of information. This interface is also customizable with the ability to visually map network components and links, further easing the process of monitoring and finding errors.

Despite the complexity and variety of information provided by Orion, the program is still easy to use. As discussed above, SNMP only provides the messaging format used in a network management system; individual devices must still be configured to work with a particular management system. So, Orion includes auto-discovery and auto-configuration features that simplify the process of adding network devices to be monitored. This is only a brief overview of Orion. Complete details of the Orion Network Performance Monitor can be found at [4].

3.2 Passive Capture Tool: Ethereal

Ethereal is an open source packet capture tool for Ethernet networks that captures packets off of network interface cards for analysis. Although Ethereal does not calculate performance statistics on captured traffic, it does analyze individual packets and determines their type as well as values of fields specific to individual protocols. It also provides filtering of packets based on protocol as well as other characteristics such as addresses and port numbers [5].

Ethereal is a two-piece software program available on the Windows, Mac and Unix operating systems. A capture library enables Ethereal to capture packets off the network interface while a graphic user interface allows administrators to view and analyze captured packets.

3.3 Application and Service Monitoring: Webmetrics GlobalWatch

Webmetrics GlobalWatch provides performance and availability monitoring for a variety of web applications including static and dynamic webpages, DNS, web transactions, Java and flash applets and more. Webmetrics utilizes a network of globally distributed monitoring agents to continuously poll websites and gather performance information. This agent network allows Webmetrics to obtain performance measurements such as response time, throughput, and availability from a similar vantage point as actual users. Webmetrics customers can use this information to monitor real user experience and react to errors and performance degradation [6].

3.4 Network Flow Monitoring: Cisco IOS NetFlow

Cisco IOS NetFlow is a complete network monitoring system used to collect and analyze network flows. NetFlow relies on routers to collect information on network flows which are identified as packet sequences that share the same IP protocol and source and destination addresses and ports. Flow information from all network devices is sent to a NetFlow collector to be analyzed. Cisco's IOS NetFlow application uses this NetFlow information to provide a variety of information and services including user and application monitoring, network planning, traffic engineering, usage accounting, and security analyzing [7]. Compared to an SNMP-based monitoring platform, NetFlow is able to give a much more detailed view of the network user behavior and usage patterns.

Though originally developed by Cisco, other network equipment vendors support NetFlow in their products. IEFT has even created an RFC for IP Flow Information eXport (IPFIX) which is based off of Cisco's NetFlow version 9 [8]. Not all network administrators need the detailed network view provided by a flow monitoring tool; however, NetFlow is becoming a much more common tool in the network administrator's toolbox

4.0 Summary

Network performance monitoring is an important part of network functionality. Society has become dependent on networks and their ability to perform optimally is crucial. As a result, numerous network performance monitoring tools have emerged. Many of these are based on the standardized management protocol SNMP and provide

Manuscript received July 5, 2007
Manuscript revised July 25, 2007

administrators a complete view of a network and it performance.

SNMP provides the messaging capability for management systems to collection network data for analysis. First introduced in 1988, SNMP is now in its third version and provides a secure messaging format. SNMP monitoring tools are some of the most flexible and comprehensive because of their ability to selectively poll any network device for exactly the information they need. SolarWind's Orion Network Performance Monitor is one example of an SNMP-based performance monitoring tool.

However, many other types of tools are also available. Ethereal provides a tool for capturing and analyzing individual packets off of a network. Webmetrics GlobalWatch is an application performance monitoring tool that utilizes distributed agents to continuously monitor the performance of web applications. And finally, network flow monitoring tools provide an increasingly popular means of monitoring network performance. Cisco's NetFlow architecture provides flow monitoring, aggregation, and analysis and has even gone to IETF as an Internet draft. As the trend towards higher performance networks continues, more comprehensive monitoring tools like NetFlow will become as commonplace as SNMP today.

References

[1] Raj Jain Network Traffic Monitor : ww.cse.wustl.edu/%7Ejain/cse567-06/ftp/net_traffic_monitors2/index.html#Jain91
[2] Packet Sniffer : http://www.packetsniffer.org
[3] Performance Tools: http://dast.nlanr.net/NPMT
[4] Orion Network Performance Monitors : http://www.extralan.co.uk/products/Diagnostic-tools/Solarwinds/orion.htm
[5] Ethereal : http://www.ethereal.com
[6] Webmatrics Global Watch: http://www.webmetrics.com
[7] Cisco IOS Netflow: http://www.cisco.com/warp/public/732/netflow
[8] Cisco Systems Netflow Version 9: http://www.ietf.org/rfc/rfc3954.txt

Nagaraja G. S, Senior Lecturer in the Department of Computer Science & Engg, R.V. College of Engineering, Bangalore. He is pursuing his doctoral programme at Dr. M.G.R University, Chennai. He obtained his M.E. degree in Engineering Management from Mysore University and BE in Computer Science from Bangalore University. His research interests are Computer Networks, Networks Management & Computer Architecture. He has guided several Under Graduate and Post Graduate projects and has published few papers in National and International conferences. Currently he is teaching courses on Computer Networks, Computer Architecture, Operating System and Advanced Microprocessor.

Ranjana Ramesh Chittal received the B.E. degree from Visvesvaraya Technological University in 2003. After working as a lecturer (from 2003) in the Department of Computer Science & Engineering, Maratha Mandal's Engineering College, Belgaum, she has been pursuing Master of Technology at R.V. College of Engineering , Bangalore under Visvesvaraya Technological University since 2006. Presently she is persuing her internship at Mindtree Consulting Ltd, Bangalore under the guidance of **Prof. B.I. Khodanpur,** HOD, Dept of CSE, RVCE, Bangalore**.** Her research interest includes Wireless Networks, Image Processing, Predictive Text Mining, etc. She has published paper in IEEE – ICSNC 2007, FISAT,etc.

Kamod Kumar received the B.E. degree from Visvesvaraya Technological University in 2003. After working as a lecturer (from 2003) in the Department of Computer Science & Engineering, Maratha Mandal's Engineering College, Belgaum, he has been pursuing Master of Technology at R.V. College of Engineering , Bangalore under Visvesvaraya Technological University since 2006. Presently he is pursuing his internship at ZTE India R&D Center Pvt. Ltd , Bangalore under the guidance of **Prof. B.I. Khodanpur,**HOD, Dept of CSE, RVCE, Bangalore. His research interest includes Wireless Networks, Value Added Services, 3G Networks,, etc. He has published paper in IEEE –ICSNC 2007, FISAT, etc.