# Management of Networks Using SNMP

**Prakash S. Teltumde**
pst205@gmail.com

**Dr. B.B. Meshram**
bbmeshram@vjti.org.in

**T. M. Bansod**
tmbansod@gmail.com

***Abstract*** **- The increasing size of network makes the management of network more and more difficult. Management of network is a very difficult task. Traditional centralized design monitoring system do not scale to provide present day , large ,complex, network computing system. This paper is a survey which aims to explain and design the Network Monitoring software which allow us to monitor the network easily and efficiently. The network management system should completely automate the manual monitoring of network system for the administrator of the network. Moreover, after detecting the system which is not responding to the network, the software will mail the administrator of that system to reset the system so that the entire network will be load free and network can work smoothly.**

***Key Words*** **- SNMP, OSI and TCP/IP, CMIP, MBI, SMI, NETMON.**

## INTRODUCTION

Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance and provisioning of networked systems. Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.

Administration deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.

Maintenance is concerned with performing repairs and upgrades - for example, when equipment must be replaced, when a router needs a patch for an operating system image, when a new switch is added to a network. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters. Provisioning is concerned with configuring resources in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.

*Network management* usually refers to the management of a network's physical infrastructure: hubs, switches, routers, and gateways. It can formally be defined as the controlling of a complex data network so as to maximize its efficiency and productivity that involves active and passive monitoring of network resources for the purpose of troubleshooting, detecting potential problems, improving performance, documentation, and reporting.

The International Organization for Standards has defined Network Management as consisting of five key areas. These areas and their underlying functions are listed below:

- *Fault Management* - Detects and corrects faults in the network.
- *Configuration Management* - Views and manages system resources and management information.
- *Security Management* - Detects and corrects faults in the network.
- *Performance Management* - Monitors and tunes network performance
- *Accounting Management* - Monitors and charges for network usage.

## OSI SEVEN LAYER MODEL AND TCP/IP MODEL RELATIONSHIP

In information technology, a protocol (pronounced PROH-tuh-cahl, from the Greek *protocollon*, which was a leaf of paper glued to a manuscript volume, describing its contents) is a special set of rules that apply to both of the end points of a telecommunication connection when they communicate. Protocols exist at several levels in commonly accepted seven-layer model of a telecommunication connection and the TCP/IP model shown in Figure 1. Both end points within these models must recognize and observe a protocol.

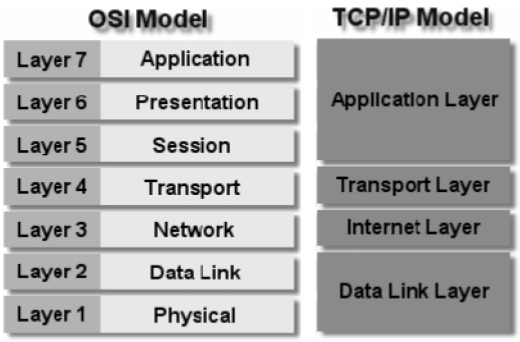



Fig. 1.1. OSI Seven Layer Model and TCP/IP Model Relationship

## COMMON NETWORK MANAGEMENT PROTOCOLS

Protocols are often described in an industry or international standard. Some of the common network management protocols, their acronyms and what functions they perform are illustrated in Table 1.

*Table 1: Network Management Protocols*

*Transmission Control Protocol/Internet Protocol (TCP/IP)*

A set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks.

*Simple Network Management Protocol(SNMP)*

SNMP enables managers to ask agents to retrieve and change information about network devices. Because SNMP has low network overhead, it is an inexpensive way to gather network statistics. It is also ideal for real-time monitoring.

*Common Management Information Protocol(CMIP)*

CMIP was designed to manage OSI networks, but it can also be used in other kinds of networks.

*Common Management Information Protocols over TCP/IP (CMOT)*

CMOT can monitor and manage networks that use the CMIP protocols in combination with TCP/IP.

*Open Systems Interconnection(OSI)*

An open system is one that complies with industry-wide standards for communication. Open systems can be connected to other open systems that comply with the same standards.

*Desktop Management Interface(DMI)*

DMI is used to manage PC and server systems.

## SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

SNMP has achieved widespread acceptance. SNMP was derived from its predecessor SGMP (Simple Gateway Management Protocol) and was intended to be replaced by a solution based on the CMIS/CMIP (Common Management Information Service/Protocol) architecture. This long-term solution, however, never received the widespread acceptance of SNMP. SNMP is based on the manager/agent model consisting of an SNMP manager, an SNMP agent, a database of management information, managed SNMP devices and the network protocol. The SNMP manager provides the interface between the human network manager and the management system. The SNMP agent provides the interface between the manager and the physical device(s) being managed. SNMP was made with one design in mind… to be simple. SNMP is a simple protocol that can be used on just about any networking device in use today. In some environments it's used heavily, in others it's scarce. SNMP is commonly used to manage devices on a network.

The SNMP protocol operates at the application layer (layer 7) of the OSI model. It specified (in version 1) five core protocol data units (PDUs):

- ✓ GET REQUEST, used to retrieve a piece of management information.
- ✓ GETNEXT REQUEST, used iteratively to retrieve sequences of management information.
- ✓ GET RESPONSE, retrieve response.
- ✓ SET, used to make a change to a managed subsystem.
- ✓ TRAP, used to report an alert or other asynchronous event about a managed subsystem.

SNMP is a tool (protocol) that allows for remote and local management of items on the network including servers, workstations, routers, switches and other managed devices. SNMP network management consists of four parts:

- ➢ Management Information Base (MIB)
  A map of the hierarchical order of all managed objects and how they are accessed.
- ➢ Structure of Management Information (SMI)
  Rules specifying the format used to define objects managed on the network that the SNMP protocol accesses.
- ➢ SNMP Protocol
  Defines format of messages exchanged by management ystems and agents.
  Specifies the Get, GetNext, Set, and Trap operations.
- ➢ Security and administration capabilities
  The addition of these capabilities represents the major enhancement in SNMPv3 over SNMPv2

The first RFCs for SNMP, now known as Simple Network Management Protocol version 1, appeared in 1988.

## SNMP VERSUS CMIP

The basic difference between the CMIP and SNMP is in design philosophy. SNMP is based on a minimalist approach embodied by Marshall Rose, one of the SNMP gurus, in the statement that "the impact of adding network management to managed nodes must be minimal, reflecting the lowest common denominator". It is the simple effectiveness of SNMP that has lead to its wide spread implementation

coupled with the collective purchasing power of Internet sites. CMIP is much more detailed and coupled with application level activities and complex network management requirements. As stated early this also applies to the use of datagram protocols for SNMP versus connection Orientated protocols for CMIP.

It is interesting to note that one of the latest suggestions for CMIP in the LAN network management standards arena is to use a level 2 protocol and hence datagram like.

CMIP does not have a GET NEXT capability, it only has a GET. CMIP also has a complex scoping and filtering mechanism to identify object instances, whereas SNMP has a direct naming approach. To get the next object SNMP asks, through GET NEXT, get me the object after the one named, which is usually the one just retrieved. In this way a table can be retrieved simply.

The equivalent operation in CMIP requires the use of the scope and filter operations. These can be hidden from the user but they do add significantly to processing requirements.

## IMPROVEMENTS IN THE PERFORMANCE OF SNMP

With the evolution of management systems and the growth in the size and complexity of MIBs there is a need to improve the efficiency of the base protocol, but without changing it! Two techniques are under discussion that can increase efficiency further. They are pipelining and the Parallel Algorithm.

Pipelining invokes multiple threads of GET NEXT operations within the manager targeted at one agent. The agent processes each request as it is received. Unaware of the fact, that the request is part of a greater scheme. The manager does not have to wait for the response to the preceding request before firing off the next. The increase in efficiency comes from the fact that the latency of the round-trip delay is eliminated. The Parallel Algorithm goes one step further, grouping the request (threads) into single SNMP operations. Whilst reducing traffic, this process increases the load on the server. Some form of flow control, based on round trip time and timeouts, is implemented by both techniques, as SO not to overrun the agent with request.

### *How SNMP is used*

SNMP is a protocol designed to manage TCP/IP networks. It gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events. SNMP is composed of 3 elements: the MIB (management information base), the manager, and the agent. SNMP is used to manage a variety of network resources including hardware products such as servers, printers, PCs, or networking products, or software such as the Windows NT operating system or a database application. Using SNMP management systems, network administrators can browse the configuration of a device, monitor collected variables such as network packet counts, or receive SNMP "traps", a message sent from the agent to the manager when an "event", such as a power failure occurs in a system.

### *What Is NetMon?*

NetMon is a program that runs on a server and tests for connectivity to the server's interfaces. It must be configured for the local network and must have some external devices to be able to contact, to enable the testing to take place.

NetMon has no kernel module components and runs completely in user space but for most configurations must be run with root level privileges to enable the program to attach to the correct internal components when running.

NetMon can be configured to operate at different speeds, with detection and switch over of traffic occurring in less than 5 seconds. In some installations it is safe to configure NetMon to respond in sub-second times but this should be used with caution as it increases the likelihood of a false, failure detection on a machine with diminishing resources (CPU etc).

### *How Does NetMon Work?*

In principle NetMon needs to send a request and receive a response and both request and response should traverse the same desired path to enable NetMon to establish if the 'path' is functioning correctly. A number of different possible techniques can be used to test connectivity, some routable and some non-routable.

In the event of a failure of the interface, or other component, then the NetMon program should, if possible, switch the traffic to another interface. NetMon will continue to test all interfaces but will only switch traffic in the event that the active interface fails.

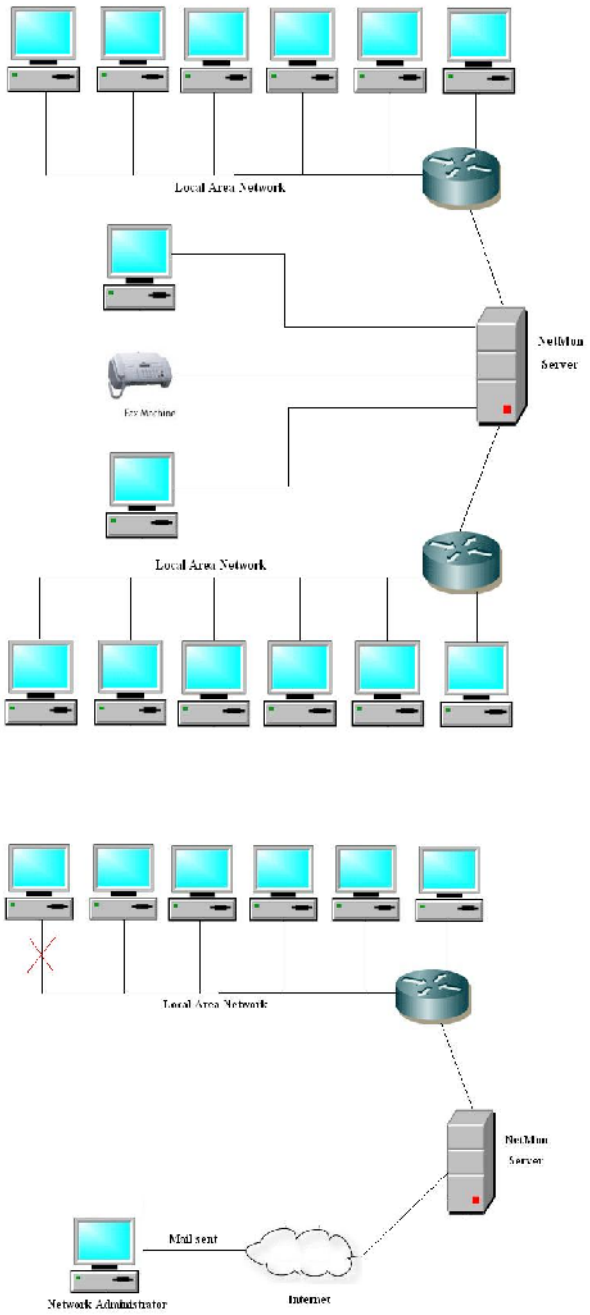
All methods allow multiple remote servers to be tested so that NetMon does actually reduce the number of single points of failure

## PHYSICAL IMPLEMENTATION

When Net-Mon is to be implemented on server machine the following pre-requisites must be satisfied.

- Management and Monitoring tools – Windows Component Wizard
- Runtime java environment
- JDK 1.1.x from Sun Microsystems

Following diagram explains how our software works in a network:




As an interface goes down NetMon sends a mail to the network administrator

## CONCLUSION

This paper describe the importance of managing the networks thought managing is critical, also describe the brief study of SNMP, along with it NETMON tool is been presented which gives idea that when tool installed on the server how the software works and describe the monitoring of the system being connected and flashes out the system which is not working so the administrator can take possible steps and helps in smooth functioning of the network.

## REFERENCES

[1] On designing SNMP based monitoring systems Supporting ubiquitous access and real-time Visualization of traffic flow in the network, using low cost tools Ranganai Chaparadza
[2] Research and Design of Network Servers Monitoring System Based on SNMP Zhen-qi WANG, Yue WANG, Guangqiang SHAO
[3] A Novel Framework of Secure Network Management for Wireless and Mobile Networks Yonglin Ren and Azzedine Boukerche, Lynda Mokdad
[4] Development of Network Management Console: SNMP based Network Mapping and Fault Management Ahmad Ashrif bin A Bakar, Norshamsun bin Ali B Hashim, Norashidah bin Md Din, Md Zaini bin Jamdudin, and Mohd Hazli bin Mohamed Zabil.
[5] A Network-Oriented Power Management Architecture Luis F. Poll0 And Ingrid Jansch-P6rto.
[6] Study of Network topologies Discovery in IP networks Yao Zhoa
[7] Network Topologic Discovery Based On SNMP Kuangyu Qin1, Chunquan Li2.
[8] Securing SNMP Across Backbone Networks H. Erik Hia and Scott F. Midkiff
[9] A Formal Approach To Model Snmp Network Management Systems Jianxin Li and Benjamin J. Leon
[10] An Architecture Of Internetworking System For Different Management Networks Tae-Soo Kim, Kwang-Hui Lee
[11] Using Snmp To Manage Networks Peter Drake

## AUTHOR'S PROFILE

**Prakash S. Teltumde**
pst205@gmail.com

**Dr. B.B. Meshram**
bbmeshram@vjti.org.in

**T. M. Bansod**
tmbansod@gmail.com