**SNMP: Protocol analysis and applications**

Kanishka Soni   
Undergraduate Student

Department of **Computer ScienceEngineering  
Mukesh Patel Institute of Management and Technology, NMIMS**

Mumbai 400056, India   
Vaibhav Soni  
Undergraduate Student

Department of **Computer ScienceEngineering  
Mukesh Patel Institute of Management and Technology, NMIMS**

Mumbai 400056, India

Tarun Tanmay  
Undergraduate Student

Department of **Computer ScienceEngineering  
Mukesh Patel Institute of Management and Technology, NMIMS**

Mumbai 4000 56, India

Snehil Suman  
Undergraduate Student

Department of **Computer ScienceEngineering  
Mukesh Patel Institute of Management and Technology, NMIMS**

Mumbai 400056, India

Vaishnavi Singh Suroth  
Undergraduate Student

Department of **Computer ScienceEngineering  
Mukesh Patel Institute of Management and Technology, NMIMS**

Mumbai 400056, India

***Abstract***— Simple Network Management Protocol (SNMP) is a framework used for managing devices on the internet and provides a set of operations for monitoring and controlling the internet. It is one of the most well-known protocols for overseeing and observing organization segments. It has complex however incredibly helpful functionalities, permitting network overseers to get network gadgets to speak with one another paying little mind to the sort of equipment utilized or the product they run. SNMP is an application-layer protocol for the trading of data between network gadgets. It's characterized by the Internet Architecture Board and is essential for the TCP/IP (Transmission Control Protocol/Internet Protocol) suite. The SNMP definition is up by the Internet Engineering Task Force (IETF). It is upon a noteworthy cluster of equipment, including secret passages, switches, switches, entryways, scanners, printers, and even Information of Things (IoT) gadgets. The growing dependence on networks for everyday tasks has created the demand for high performance; reliable systems are thereby making companies invest a lot on research on improving the structures 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 systems. The most common class of devices is on the Simple Network Management Protocol, for sending and transmitting network performance information on IP networks.

This protocol has two essential components: SNMP agents and SNMP managers. Management is not achieved only through the SNMP protocol but by the assistance of two other protocols at the application layer level: Management Information Base (MIB) and Structure of management information (SIM). Moreover, SNMP designs are deployed on a large number of network devices, have minimal impact and transport requirements on the managed nodes, and continue working when most other network applications fail.

Keywords- SNMP, SNMP agents, SNMP managers, IETF, MIB, SIM.

# **INTRODUCTION**

SNMP is a framework for managing devices in an internet using the TCP/IP protocol suite. It uses the concept of manager and agent. SNMP is an application-level protocol and is designed at that level so that it can monitor devices made by different manufacturers and installed on other physical networks. The SNMP finds its usage in heterogeneous networks made up of various Local Area Networks and Wide Area Networks connected by routers made by different manufacturers.

# **MANAGERS AND AGENTS**

The simple action between managers and agents helps in establishing management.

## Managers

A manager is a host that runs the SNMP client program. It hosts and monitors agents. The manager can access all the values in a database, and it can fetch and compare the costs of variables from a router that it connects. A manager can also make the agent perform a certain number of actions.

SNMP Manager's essential functions:

* Queries agents
* Gets responses from agents
* Sets variables in agents
* Acknowledges asynchronous events from agents

## Agents

An agent or a management station is a host that runs the SNMP server program. An agent keeps performance information in a database. They contribute to the management process to a great extent, especially with warning messages.

Critical functions of SNMP's agents:

* Collects management information about its local environment
* Stores and retrieves management information as defined in the MIB.
* Signals an event to the manager.
* Acts as a proxy for some non–SNMP manageable network node.

# **MANAGEMENT AND NETWORK MANAGEMENT COMPONENTS**

SNMP management is on the following basis:

### A manager checks an agent by requesting information that reflects the behaviour of the agent.

### A manager forces an agent to perform a task by resetting values in the agent database.

### An agent contributes to the mangement process by warning the manager of an unusual situation.

## Structure of Management Information(SMI)

SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values.

Its functions are:

* To name objects
* defining the type of data which can is stored in an item
* To show how to encode data for transmission over the network.

It emphasizes on three attributes to handle an object: name, data type, and encoding method.

### Name

To name objects globally, SMI uses an object identifier. An object identifier (OID) is a tag that allows a management entity to refer unambiguously to a particular item. The allocation of object identifiers is in a tree fashion. The value of the object identifier is a sequence of integers that refer to a specific traversal of the object tree.

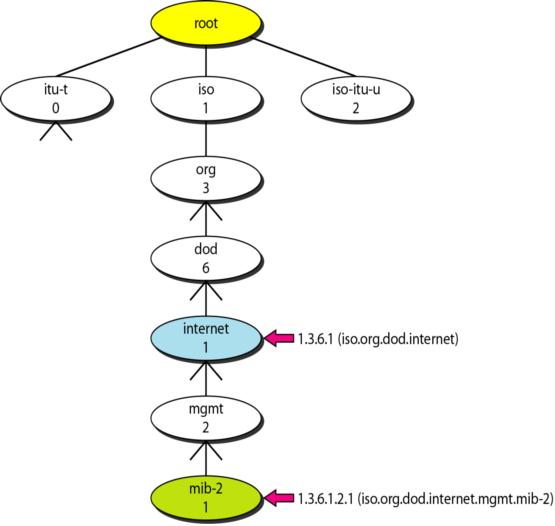


Fig 1: Object Identifier hierarchy

The tree structure starts with an unmade root. Each object can be defined using a sequence of integers separated by dots. SNMP uses integer dot representation. The people use the name-dot picture.

For example:

iso.org.dod.internet.mgmt.mib-2 🡨🡪 1.3.6.1.2.1

### Type

To define a data type, SMI uses Abstract Syntax Notation One (ASN.1) definitions and adds some new illustrations. SMI has two broad categories of data types: simple and structured.

#### Simple Type

The simple data types are atomic data types which are from ASN.1: SMI adds some.

#### Structured Type

By combining simple and structured data types, we can make new structured data types

SMI defines two structured data types:

* Sequence: A sequence data type is a combination of simple data types, not necessarily of the same kind.
* Sequence of: The sequence of a series of data type is a combination of simple data types all of the same type or a variety of sequence data types all of the same kind.

### Encoding Method

SMI uses another standard, Basic Encoding Rules (BER), to encode data to be transmitted over the network. BER specifies that each piece of data is encoded in triplet format: tag, length, and value. The title is a one-byte field that defines the type of data. The length field is one or more bytes. If it is 1 byte, the most significant bit must be 0.the other 7 bits define the length of the data.

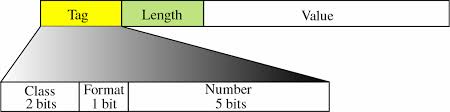


Fig 2: An Encoding format

## Management Information Base(MIB)

MIB creates a collection of named objects, types, and their relationships to each other in a manageable entity. Each agent has its own MIB, which is a collection of all the items a manager can handle.

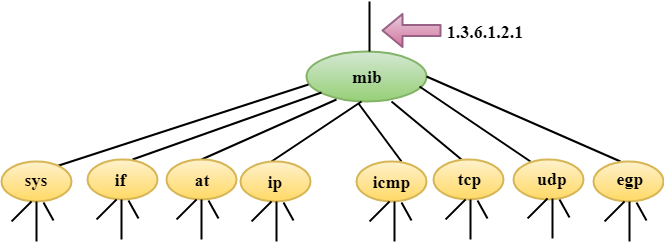


Fig 3: objects in MIB

The following is a brief description of some of the objects:

* **sys**: This object (system) represents general information about the node(system), such as the name, location, and lifetime.
* **if**: This object (interface) defines information about all of the interfaces of the node, including interface number, physical address, and IP address.
* **at**: This object (address translation) defines the information about the ARP table.
* **ip**: This object represents information related to Internet Protocol, such as the routing table and the Internet Protocol address.
* **icmp**: This object defines information related to Internet Control Message Protocol, such as the number of packets sent and received and total errors created.
* **tcp**: This object defines general information associated with Transfer Control Protocol, such as the connection table, timeout value, number of ports, and number of packets sent and received.
* **egp**: These objects are related to the operation Exterior Gateway Protocol.
* **trans**: These objects are associated with the specific method of transmission.
* **snmp**: This object defines general information related to SNMP itself.

## Simple Network Transfer Protocol(SNMP)

It has a particular role in network management. It defines the format of the packet which is sent by the manager to the agent and vice versa. It also interprets the result and creates statistics. SNMP defines the structure of packets exchanges between a manager and an agent. It reads and changes the status of objects (values of variables) in SNMP packets.

It is an application that allows:

* A manager to retrieve the value of an object defined in an agent.
* A manger to store a value in an object defined in an agent.
* An agent to send an alarm message about an abnormal situation to the manager.

SNMP works by sending messages, called protocol data units (PDUs), to devices within the neighbouring network that "speak" SNMP. These messages are called SNMP Get-Requests. Using these requests, network administrators can track virtually any data values they specify. The information which is tracked by SNMP gets sent to the product that asks for it. That product can either display or store the data, depending on an administrator's preferences.

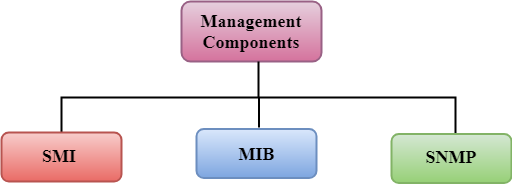


Fig 4 :SNMP Management Components

# **PROTOCOL DATA UNITS**

## GetRequest

The Protocol Data Unit (PDU) retrieves the value of a variable or a set of variables. The manager and the agent send PDU to each

## GetNextRequest

The GetNext PDU allows a manager to request the next sequential object in the MIB.

## GetBulkRequest

This PDU is sent from the manager to the agent to retrieve a large amount of data.

## SetRequest

A manager sends a Set message to an agent to change the value held by a variable on the agent. It finds its usage in control configuration information, or it otherwise modifies the state of remote hosts. It is the only write operation defined by the protocol.

## Response

This message, sent by an agent, is used to send any requested information back to the manager. It serves as transport for data requested, and acknowledgement of receipt of the request. When the requested data doesn't return, the response contains error fields that get set with further information. A response message returns for any of the above requests, as well as Inform messages.

## Trap

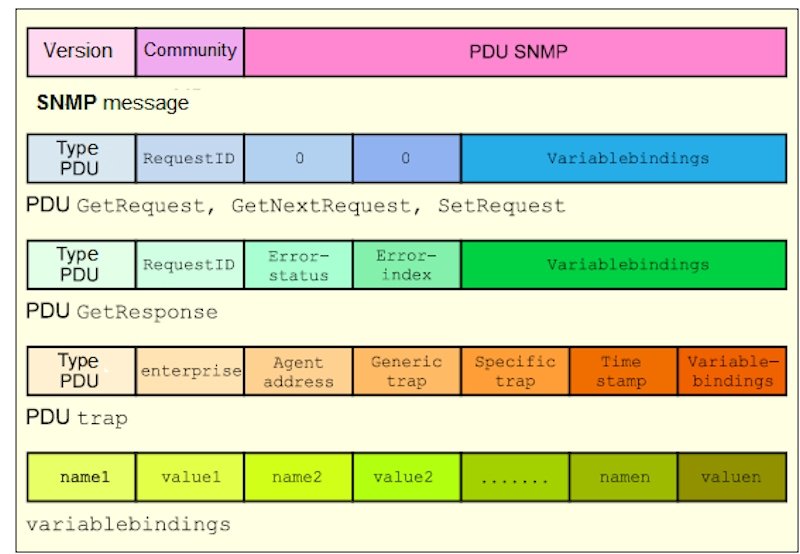
An agent generally sends a trap message to a manager. Traps are asynchronous notifications in that they are unsolicited by the manager receiving them. They are mainly used by agents to inform managers of events that are happening in their managed devices.

## InformRequest

The InformRequest PDU is sent from one manager to another remote manger to get the values of some variables from agents under the control of the private manager.

## Report

The Report PDU reports some types of errors between managers. It is not yet in use.

  
Fig 5: SNMP PDU format

# **SNMP VERSIONS**

## SNMPv1

It was the first implementation, operating within the structure management information specification, and described in Request for Comments (RFC) 1157. It uses community strings for authentication and UDP only.

## SNMPv2

This version has improved support for efficiency and error handling and is described in Request for Comments (RFC) 1901. It was first introduced in RFC 1441 and is more appropriately known as SNMP v2c. Its uses are for UDP, but it gets configured to operate with TCP.

## SNMPv3

Version 3 of the protocol made its debut in 1998, made more significant strides to securing the protocol suite by implementing the "user-based security". It uses TCP and improves security and privacy; introduced as in RFC 3410. Therefore, the higher the version of SNMP, the more secure it will be.

# **SECURITY LEVELS**

The Security levels usage is in the only SNMPv3. There are three security levels, namely:

## noAuthNoPriv

This (no authentication, no privacy) security level uses community string for authentication and no encryption for privacy.

## authNopriv

This security level (authentication, no privacy) uses HMAC with Md5 for authentication, and no encryption is there for privacy.

## authPriv

This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses DES-56 algorithm.

# **SNMP FEATURES**

|  |  |
| --- | --- |
| **Feature** | **Example** |
| Expanded data types | 64-bit counters |
| Improved efficiency and performance | get-bulk operator |
| Confirmed event notifications | inform operator |
| Richer error handling | errors and exceptions |
| Improved sets | row creation/deletion |
| Fine-tuned data definition language | SMI, textual conventions, conformance statements, and agent capabilities |

# **Security Mechanisms**

1. MD5 message-digest algorithm in HMAC
   1. Directly provides data integrity checks
   2. Indirectly includes data origin authentication
   3. Uses a private key known by sender and receiver
   4. 16-byte key
   5. 128-bit digest (truncates to 96 bits)
2. SHA, an optional alternative algorithm
3. Loosely synchronized monotonically increasing time indicator values defend against specific message stream modification attacks
4. The User-Based Privacy is on the following basis:
5. Data Encryption Standard (DES) Cipher Block Chaining (CBC) mode
   1. Provides data confidentiality
   2. Uses encryption
   3. Subject to export and use restrictions in many jurisdictions
6. Uses 16-byte key (56-bit DES key, 8-byte DES initialization vector) known by sender and receiver
7. Multiple levels of compliances concerning DES due to problems associated with international use
8. Triple Data Encryption Standard (Triple DES)
9. Advanced Encryption Standard (128, 192, and 256, bit keys)

# **Security Threats and SNMPv3 Protection**

|  |  |
| --- | --- |
| **Threat** | **SNMPv3 Protection** |
| Masquerade | Verifies the identity of the message's origin by checking the integrity of the data. |
| Modification of Information | Thwarts accidental or intentional alterations of in-transit messages by checking the integrity of the data, including a timestamp. |
| Message Stream Modification | Thwarts replay attacks by checking message stream integrity, including a time stamp. |
| Disclosure | Prevents eavesdropping by protocol analysers, etc., by using encryption |
| Unauthorized Access | Verifies operator authorization and protects critical data from intentional and/or accidental corruption by using an access control table (part of policy-based management). |

# **configuration**

## **SNMP configuration**

1. Click Start, go to Control Panel, then in Administrative Tools go to Computer Management.
2. In the console tree, click Services. In the right pane, double-click SNMP Service.
3. Type the name of the user or administrator of the computer in the Contact box, and then type the physical location of the computer or contact in the Location box.
4. Under Service, click to select the checkboxes next to the services that are provided by the computer. Service options are:
   * Physical: Specifies whether the computer manages physical devices, such as a hard disk partition.
   * Applications: Specifies whether the computer uses any programs that send data by using TCP/IP.
   * Datalink and subnetwork: Specify whether this computer manages a TCP/IP subnetwork or data link, such as a bridge.
   * Internet: Specifies whether this computer acts as an IP gateway (router).
   * End-to-end: Specifies whether this computer acts as an IP host.
5. Under Trap destinations, click Add. In the Hostname, IP or IPX address box, type the name, IP or IPX address of the host, and then click Add. Repeat these steps to add the communities and trap destinations that one wants.
6. Click to select the Send authentication trap checkbox if one wants a trap message sent whenever authentication fails.
7. Under Accepted community names, click Add. To specify how the host processes SNMP requests from the selected community, connect the permission level that one wants in the Community Rights box.
8. Specify whether or not to accept SNMP packets from a host. For this:
   * To accept SNMP requests from any host on the network, regardless of identity, click Accept SNMP packets from any host.
   * To limit the acceptance of SNMP packets, click.  
     Accept SNMP packets from these hosts, click Add, and then type the appropriate hostname, IP or IPX address in the Hostname, IP or IPX address box.
9. Click OK

## **Implementation**

## The SNMP's powerful writing capabilities that allow configuration of network devices are not utilized by the vendors thoroughly. It is due to a scarcity of security in SNMP versions before SNMPv3, and partly because many devices aren't capable of being configured via individual Management Information Base object changes. Most SNMP implementations, regardless of which version of the protocol they support, use an equivalent program code for decoding protocol data units (PDU), and the problems identified during this code. Many vendors had to issue patches for their SNMP implementations.

## **Configuration Methods**

SNMP gets configured through the following methods:

* SL3000 and SL8500: CLI (Command Line Interface)
* SL500: CLI and the SL (StorageTek Library) Console
* SL150: SL150 GUI (Graphical User Interface) with the user role of either administrator or service

## **Configuration requirements**

The following are configuration requirements:

1. Firmware for StorageTek Modular Libraries must be:
   * SL8500: version FRS\_3.12 or higher
   * SL3000: version FRS\_1.7 or higher
   * SL500: version FRS\_1067 or higher
   * SL150: version FRS\_1.0 or higher
2. The SL Console must be version FRS\_4.0 or higher.
3. By default, the SNMP agent is disabled and must be enabled.
4. STA (Single Tank Adapter) has different firmware requirements. See the STA documentation for more information.

# **types of monitoring tools**

## **Passive Analysis:**

Passive network monitoring tools make use of real applications and their traffic to record the application experience using the network. E.g.:- Grid FTP is used to record throughput of total Grid traffic across the network and with other applications. This feature is beneficial because no additional traffic introduces itself throughout the network but in the schedule will reflect the user's experience in performing specific tasks and as such might not accurately record the capabilities of the network. Also, any maintenance issues related to the monitoring aspects of applications are dependent for correction on maintainers of grid application itself.

It is a class of network tools that do not generate any traffic themselves while collecting data. They are also known as packet capture tools or packet sniffers. In the case of passive analysis, the analyser merely listens to traffic that is on the network. The breadth of the analysis generated by passive tools is fundamentally limited because they will only see the traffic which is local to the device running the analyser. E.g.:- A passive system would only see traffic sent to or from its host in a switched Ethernet environment.

## **Application and Service Monitoring:**

keep track of essential systems required to keep the network up, healthy, and to run, Application and service monitoring tools, keep track of crucial systems necessary to keep the network up, healthy and running. This tool notifies the authorized personnel and network administrators, so the problem gets fixed long before it takes out the entire system. It also works well for tracking application usage across the organization.

It is the class of performance monitoring tools that provide monitoring of individual network applications. It depends less on the network equipment and infrastructure and more on the actual servers that provide user services—reporting on utilization and performance as well as performance characteristics and application availability of the underlying server. Website availability monitoring is one everyday use for application monitoring. Other uses are built on services and protocols much more complicated than HTTP. Server load, memory and disk usage, transaction rate, and concurrent connection count are the things which database monitoring consists. To quickly identify and resolve application problems and evaluate infrastructure performance for bottlenecks or excess capacity, administrators can use this information.

## **Integrated SNMP Monitoring Platforms:**

The integrated SNMP Network Management System platform actively collects network information from network devices and analyses the data. It leverages SNMP to give a complete view of a network. SNMP network management systems provide alerts based on real-time monitoring and reporting and any of the monitored performance characteristics. Graphic reporting, administration of networks and monitoring id provided by most integrated platforms. Complete monitoring systems supply a detailed and comprehensive analysis of network performance. Bandwidth utilisation, response time, throughput, error rates, CPU load and memory utilisation of network equipment and servers are the typical performance characteristics.

## **Flow Monitoring:**

Flow-based monitoring tools can process and capture real user data. Hence you can get aggregate statistics of the protocols and users consuming a link capacity or examine a specific sequence of packets to pinpoint performance issues between client and server. A software agent, an inline device, or a network element which is switching the user traffic captures the traffic flows. For storage and processing, the captured flow gets delivered to a central collector.

Flow monitoring analyses the network traffic as flows, instead of looking at the traffic from a packet level. Based on individual connections, protocols, users, or applications, flow monitoring aggregates the network accordingly. It allows them to provide a bigger picture view of the network, which includes specific information on connection performance and Application and insight into routing and even network security. It also aids traffic engineering and network planning because flow monitoring can identify traffic trends.

Table

Description automatically generated

# **implementation of monitoring tools**

## **SNMP Implementation – Monitoring Tools:**

The Simple Network Management Protocol (SNMP) gets implemented using the monitoring tools to manage several devices connected to a network. The powerful write capabilities of the SNMP allow the configuration of network devices. SNMP monitoring tools support this capability by providing security. The SNMP protocol provides polling device MIBS to extract critical information, fix performance and availability issues, and fix monitoring issues related to hardware and software.

To monitor the manage devices, the SNMP equips network admins for access, collection, organization, and modification of the data and information related to a device's behaviour. The SNMP monitoring tools allow receiving and configuration alerts, monitoring device performance metrics, undertaking active polling and offering granularity, accuracy, and efficiency to determine network health and performance. Listed below are some best widely used SNMP monitoring tools:

**1)ManageEngine OpManager:** The processing element of this tool manages about 300 messages per second. The device stands out due to the trap receiver features it offers, including logging functions to get a comprehensive overview of all the trap processes. Any potential issue or equipment defect gets identified using the collated feedback. The ManageEngine OpManager serves as a comprehensive SNMP tool since it is compatible with the Windows and Linux platforms. It can monitor speed, latency, packet loss, discards, errors, and other critical metrics. It also allows monitoring of bottlenecks, monitors CPU, memory, and disk utilization. The tools offer to set multi-level thresholds for providing higher security and alerts on the security breach and features like network mapping, status monitoring, traffic analysis, and customizable widgets on its dashboard. This tool is also available on iOS and Android. It comes with three editions – Standard, enterprise, and Professional.

**2. Kaseya Network Monitor:** The Kaseya Network Monitor serves as one of the best SNMP monitors for Windows. It offers various features, such as the monitoring of Windows registry performance counters and the WMI queries. The platform is agentless and gets integrated with the Kaseya VSA. Its primary usage is for monitoring everything from firewalls to servers. The array of monitoring services that it offers, such as log, SNMP trap, file and directory, and mail quality-of-service monitoring, can be used to establish an ideal network management system. The system also has its scripting language, which is extremely easy to use and allows the assembly of scripts from the IDE itself.

It is also available for other operating systems and holds its ground when faced with several competitors.

**3. Pulse way IT Management Software:** The Pulse way IT Management Software allows Windows, Mac, and Linux users to enjoy monitoring features for various networking elements. It is also compatible with mobile devices and enables sending on-the-go commands, allowing users to fix issues on the go. Again, they can run commands directly in the terminal and perform actions such as restarting services, applying updates, and managing processes from their mobile device. However, even with all its benefits, Pulse way does fall short compared to various other networking monitoring tools in the market. It could improve many of its multiple features, especially the alerts systems, which currently do not offer any customization for receiving notifications.

**4. Spiceworks Network Monitor:** It is a useful free tool designed only for the monitoring of SNMP powered models. It is free software but offers a lot of features one wouldn’t expect from it. It has an incredibly user-friendly dashboard and allows them to get it set up and running within minutes. The system also enables the creation of SNMP device widgets on their dashboard for easier monitoring and configuring its various attributes. The customization feature is what offers Spiceworks a serious edge over other free SNMP managers in the market. However, if they need a sophisticated SNMP monitoring system for an extensive scale network, they would probably be better off with a more advanced and paid tool.

**5. Ipswich Whatsup Gold:** Whatsup Gold is an excellent monitoring system by the brand Ipswich. While this includes various infrastructure monitoring capabilities, its primary focus is on the monitoring and augmentation of networks. It is another excellent SNMP monitoring tool for Windows and covers versions from Windows Server 2008 to 2016. When users get started with the software, they will find its network discovery tool to be quite useful. It can show its current status information for use on another system, and it can automatically place network devices into maintenance mode before applying any permanent changes. It is incredibly supportive of integration and allows it to work with its REST API. Users can also undertake automation by inputting some information from an external system or separate script. It also overs support for Android and iOS devices. However, it also has an incredibly complicated setup which can require training to complete.

**6. Logic Monitor:**The Logic Monitor tool combines the functionalities of SNMP with NetFlow sourced data and offers a comprehensive view of the network’s performance. The NetFlow utility displays traffic flow over links, whereas SNMP keeps track of equipment status. The tool relies on a cloud-based system as it is more beneficial to combine data from multiple sites. It offers automatic device and interfaces discovery, wireless access-point monitoring, and interface metrics. It employs the software as a service approach and lets users’ access and monitor the devices from anywhere since information collating servers are located offsite. The logic monitor tool provides the SaaS feature, which is highly valued, but due to cloud-based data being vulnerable to a security breach, IT professionals have raised concerns.

## **Features and Applications of Some Monitoring Tools:**

##### 

##### **Conclusion**

A crucial part of any network management system and its network functionality is network performance monitoring. Our society has become heavily dependent on networks which makes it even more critical for them to function correctly. Several network monitoring systems are there in the market to ensure this. The build of most of these systems is using the SNMP protocol, which helps provide the admins with a new view of network performance.

The SNMP provides management systems with the ability to collect data for analysis easily. In its third version, it has grown much more advanced than it was back in 1988 at its launch. The monitoring tools based on SNMP are quite flexible and comprehensive since they can select and analyze any network device for the required information.

Such network flow monitoring tools provide an increasingly popular way for analyzing network performance. As networks continue to adapt and get more advanced, the monitoring tools will also start to evolve and get more comprehensive.

##### **ACKNOWLEDGEMENT**

Sincere gratitude and thanks to Ms Pragati Khare, the subject teacher for Computer Networks. The continuous guidance, support of our teacher in the class and otherwise have enabled us to understand and complete this research paper.

##### **References**

1. Mr G.S Nagaraja, Ranjana R.Chittal, Kamod Kumar, "Study of Network Performance Monitoring Tools-SNMP", in IJCSNS vol 7, July
2. Ahmed Hijazi, "A Step on Developing Network Monitoring Tools", Computer Engineering and Intelligence Systems, Vol 5, 2014
3. <https://support.microsoft.com/en-in/help/324263/how-to-configure-the-simple-network-management-protocol-snmp-service-i>
4. <https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol>
5. <https://docs.oracle.com/cd/E24292_01/en/E35317/html/snmpconfig.htm>
6. <https://www.poweradmin.com/blog/types-of-network-monitoring-applications/>
7. <https://www.applicationperformancemanagement.org/network-monitoring/network-monitoring-tools/>
8. <https://www.pcwdld.com/snmp-monitoring-tools-and-software>
9. <https://en.wikipedia.org/wiki/Kaseya_Network_Monitor>
10. <https://www.logicmonitor.com/>
11. <https://www.spiceworks.com/free-network-monitoring-management-software/>
12. <https://www.ipswitch.com/network-monitoring>
13. <https://www.pulseway.com/>
14. <https://netbeez.net/blog/what-tools-to-monitor-network-availability-and-performance/>