# Simple Network Management Protocol(SNMP)

**Simple Network Management Protocol (SNMP)** is an "Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

*The Simple Network Management Protocol (SNMP) is a framework for managing devices in an Internet using the TCPIIP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an Internet.*

**Concept**
SNMP uses the concept of manager and agent. That is, a manager, usually a host, controls and monitors a set of agents, usually routers . SNMP is an application-level protocol in which a few manager stations control a set of agents. The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.

**Managers and Agents**
A management station, called a manager, is a host that runs the SNMP client program. A managed station, called an agent, is a router (or a host) that runs the SNMP server program. Management is achieved through simple interaction between a manager and an agent. The agent keeps performance information in a database. The manager has access to the values in the database. For example, a router can store in appropriate variables the number of packets received and forwarded. The manager can fetch and compare the values of these two variables to see if the router is congested or not.

**An SNMP-managed network consists of three key components:**

- Managed device
- Agent — software which runs on managed devices
- Network management system (NMS) — software which runs on the manager

A ***managed device*** is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An ***agent*** is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP specific form.

A ***network management system*** **(NMS)** executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

Management with SNMP is based on three basic ideas:

1. A manager checks an agent by requesting information that reflects the behavior of the agent.
2. A manager forces an agent to perform a task by resetting values in the agent database.
3. An agent contributes to the management process by warning the manager of an unusual situation.

SNMP operates in the Application Layer of the Internet Protocol Suite (Layer 7 of the OSI model). The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response will be sent back to the source port on the manager. The manager receives notifications (Traps and InformRequests) on port 162. The agent may generate notifications from any available port.

To do management tasks, SNMP uses two other protocols:

1. Structure of Management Information (SMI)
2. Management Information Base (MIB).

**Role of SNMP**

SNMP has some very specific roles in network management. It defines the format of the packet to be sent from a manager to an agent and vice versa. It also interprets the result and creates statistics (often with the help of other management software). The packets exchanged contain the object (variable) names and their status (values). SNMP is responsible for reading and changing these values.

**Roles of SMI**

SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values. SM1 does not define the number of objects an entity should manage or name the objects to be managed or define the association between the objects and their values.

The Structure of Management Information, version 2 (SMIv2) is a component for network management. Its functions are

1. To name objects
2. To define the type of data that can be stored in an object
3. To show how to encode data for transmission over the network

SMI is a guideline for SNMP. It emphasizes three attributes to handle an object: name, data type, and encoding method .

**Roles of MIB**

For each entity to be managed, this protocol must define the number of objects, name them according to the rules defined by SMI, and associate a type to each named object .*MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed.*

Each agent has its own MIB2, which is a collection of all the objects that the manager can manage. The objects in MIB2 are categorized under 10 different groups: system, interface, address translation, ip, icmp, tcp, udp, egp, transmission, and snmp.

**Analogy:**

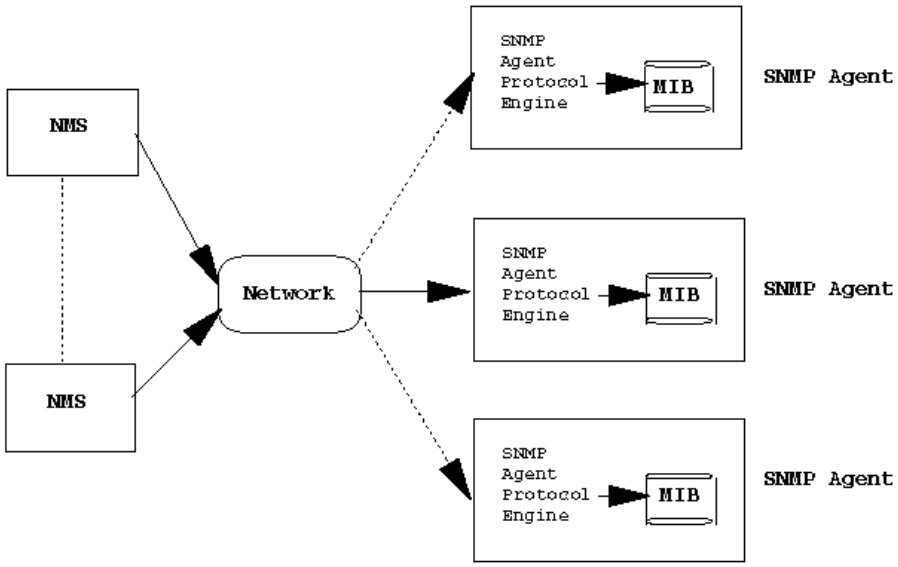
We can compare the task of network management to the task of writing a program.

- Both tasks need rules. In network management this is handled by SMI.
- Both tasks need variable declarations. In network management this is handled by MIB.
- Both tasks have actions performed by statements. In network management this is handled by SNMP.

## Network Management Architectures

Network management system contains two primary elements: a manager and agents. The Manager is the console through which the network administrator performs network management functions. Agents are the entities that interface to the actual device being managed. Bridges, Hubs, Routers or network servers are examples of managed devices that contain managed objects. These managed objects might be hardware, configuration parameters, performance statistics, and so on, that directly relate to the current operation of the device in question. These objects are arranged in what is known as a virtual information database , called a management information base, also called MIB. SNMP allows managers and agents to communicate for the purpose of accessing these objects.

**Architecture**




**A typical agent usually:**

- Implements full SNMP protocol.
- Stores and retrieves management data as defined by the Management Information Base
- Can asynchronously signal an event to the manager
- Can be a proxy (The proxy agent then translates the protocol interactions it receives from the management station) for some non-SNMP manageable network node.

**A typical manager usually:**

- Implemented as a Network Management Station (the NMS)
- Implements full SNMP Protocol
- Able to
    - Query agents
    - Get responses from agents
    - Set variables in agents

# Computer security requirements and Attacks:

Computer and network security address four requirements:

1. confidentiality: Requires that data only be accessible by authorized parties. This types of access includes printing, displaying and other forms of disclosure of the data.
2. Integrity: Requires that data can be modified only by authorized users. Modification includes writing, changing, changing status, deleting and creating.
3. Availability: Requires that data are available to authorized parties.
4. Authenticity: Requires that host or service be able to verify the identity of a user.