Simple Network Management Protocol (SNMP)

- If an organization has 1000 devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, a Simple Network Management Protocol (SNMP) is used.

Simple Network Management Protocol (SNMP)

SNMP is an application layer protocol that uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults, and sometimes even to configure remote devices.

Components of SNMP
There are mainly three components of SNMP:

1. **SNMP Manager –**
   It is a centralized system used to monitor the network. It is also known as a Network Management Station (NMS). A router that runs the SNMP server program is called an agent, while a host that runs the SNMP client program is called a manager.

2. **SNMP agent –**
   It is a software management software module installed on a managed device. The manager accesses the values stored in the database, whereas the agent maintains the information in the database. To ascertain if the router is congested or not, for instance, a manager can examine the relevant variables that a router stores, such as the quantity of packets received and transmitted.

3. **Management Information Base –**
   MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables. A MIB, or collection of all the objects under

management by the manager, is unique to each agent. System, interface, address translation, IP, udp, and egp , icmp, tcp are the eight categories that make up MIB. The mib object is home to these groups.

SNMP messages

- **GetRequest** : It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.
- **GetNextRequest :** To get the value of a variable, the manager sends the agent the GetNextRequest message. The values of the entries in a table are retrieved using this kind of communication. The manager won't be able to access the values if it doesn't know the entries' indices. The GetNextRequest message is used to define an object in certain circumstances.
- **SetRequest :** It is used by the SNMP manager to set the value of an object instance on the SNMP agent.
- **Response :** When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.
- **Trap :** These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.
- **InformRequest :** It was added to SNMPv2c and is used to determine if the manager has received the trap message or not. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.

SNMP security levels

The type of security algorithm applied to SNMP packets is defined by it. These are used in only SNMPv3. There are 3 security levels namely:

1. **noAuthNoPriv –**
   This (no authentication, no privacy) security level uses a community string for authentication and no encryption for privacy.

2. **authNopriv –** This security level (authentication, no privacy) uses HMA
3. C with Md5 for authentication and no encryption is used for privacy.

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

Versions of SNMP

There are three versions of SNMP including the below ones:

1. **SNMPv1 –**
   It uses community strings for authentication and uses UDP only. SNMPv1 is the first version of the protocol. It is described in RFCs 1155 and 1157 and is simple to set up.

2. **SNMPv2c –**
   It uses community strings for authentication. It uses UDP but can be configured to use TCP. Improved MIB structure elements, transport mappings, and protocol packet types are all included in this updated version. However, it also makes use of the current "community-based" SNMPv1 administrative structure, which is why the version is called SNMPv2c. RFC 1901, RFC 1905, and RFC 1906 all describe it.

3. **SNMPv3 –**
   It uses Hash-based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, the conclusion is the higher the version of SNMP, the more secure it will be. NMPv3 provides the remote configuration of SNMP entities. This is the most secure version to date because it also includes authentication and encryption, which may be used alone or in combination. RFC 1905, RFC 1906, RFC 2571, RFC 2572, RFC 2574, and RFC 2575.6 are the RFCs for SNMPv3.

Advantages of SNMP

- 1. It is simple to implement.
- 2. Agents are widely implemented.
- 3. Agent level overhead is minimal.
- 4. It is robust and extensible.
- 5. Polling approach is good for LAN based managed object.
- 6. It offers the best direct manager agent interface.
- 7. SNMP meet a critical need.

Limitation of SNMP

- 1. It is too simple and does not scale well.
- 2. There is no object orietned data view.
- 3. It has no standard control definition.
- 4. It has many implementation specific (private MIB) extensions.
- 5. It has high communication overhead due to polling