***Assignment No. 2***

***NAME: Ashish Mukherjee***

***ROLL NO.: 2193060***

***CLASS: LY NS***

**ASSIGNMENT 2**

**AIM-** Use SNMP to create network and list all flags.

**THEORY**-

**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, 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 used to configure remote devices.

**SNMP components –**   
There are 3 components of SNMP: 

1. **SNMP Manager –**   
   It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)
2. **SNMP agent –**   
   It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.
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.

**SNMP messages –**   
Different variables are: 

1. **GetRequest –**   
   SNMP manager sends this message to request data from the SNMP agent. 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.
2. **GetNextRequest –**   
   This message can be sent to discover what data is available on an SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, the SNMP manager can take knowledge of all the available data on SNMP agents.
3. **GetBulkRequest –**   
   This message is used to retrieve large data at once by the SNMP manager from the SNMP agent. It is introduced in SNMPv2c.
4. **SetRequest –**   
   It is used by the SNMP manager to set the value of an object instance on the SNMP agent.
5. **Response –**   
   It is a message sent from the agent upon a request from the manager. When sent in response to Get messages, it will contain the data requested. When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.
6. **Trap –**   
   These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.
7. **InformRequest –**   
   It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to send trap message continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn’t provide.

**SNMP security levels –**   
It defines the type of security algorithm performed on SNMP packets. 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 HMAC 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.

**SNMP versions –**   
There are 3 versions of SNMP: 

1. **SNMPv1 –**   
   It uses community strings for authentication and uses UDP only.
2. **SNMPv2c –**   
   It uses community strings for authentication. It uses UDP but can be configured to use TCP.
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.

**CONCLUSION**-

We have listed all the flags of SNMP