Simple Network Management Protocol (SNMP):

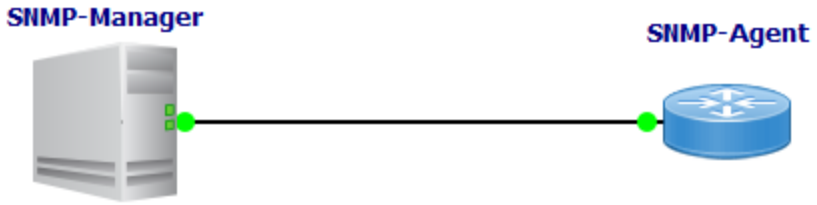
- SNMP is term which is stands for Simple Network Management Protocol.
- SNMP is used to monitor and manage devices on your whole networks.
- It has several uses, from monitoring & generating alerts to device configuration.
- Simple Network Management Protocol (SNMP) is the application layer protocol.
- SNMP is the key protocol used to retrieve information from the network devices.
- SNMP is used to retrieve information from routers, switches & network servers etc.
- SNMP can be configured as Read-Only mode to retrieve only information from devices.
- SNMP Read-Write mode can be used to retrieve or configure the network devices.
- All SNMP messages are transported via User Datagram Protocol (UDP).
- SNMP agent receives requests on User Datagram Protocol (UDP) port 161.
- SNMP Traps, information to the manager over Port User Datagram Protocol UDP 162.

SNMP Manager:

- A software that runs on the device of the Network administrator System.
- A Computer to monitor network, also called Network Management System.

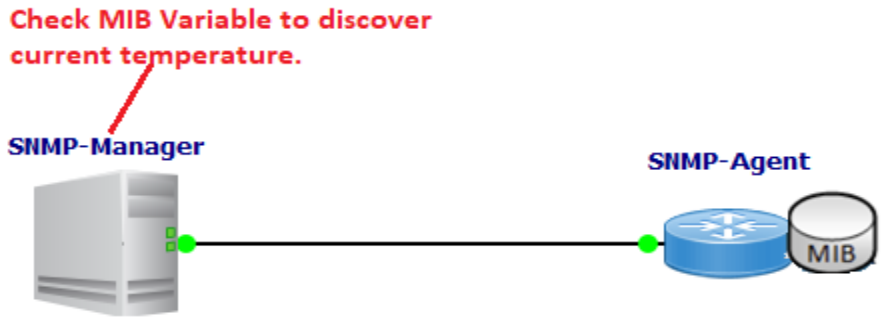
SNMP Agent:

- A software runs on network devices that we want to monitor router, firewall, etc.



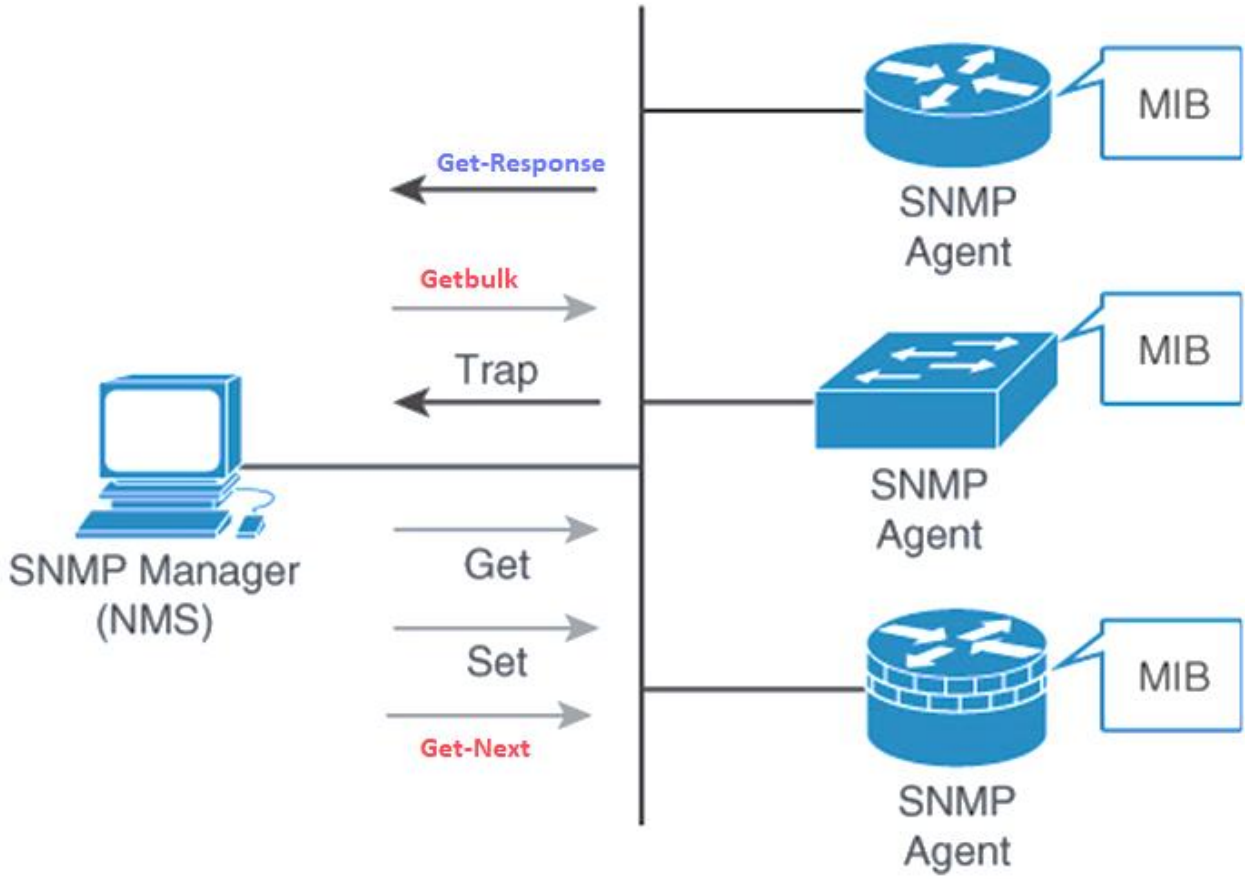
Management Information Base (MIB):

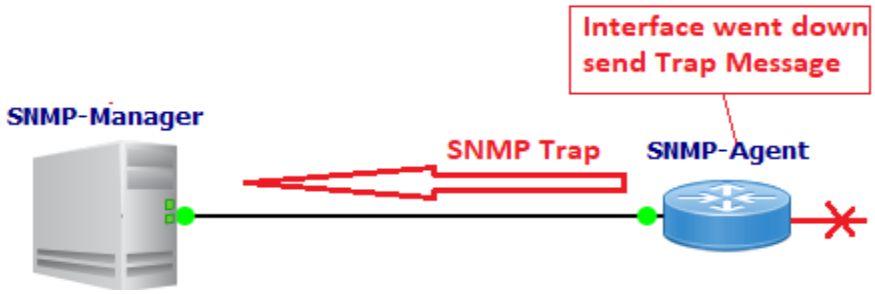
- Management Information Base (MIB) is the collection of managed objects.
- MIB contains a set of questions that the SNMP Manager can ask the Agent.
- MIB contains a set of questions that the Agent can understand them.
- MIB is commonly shared between the Agent and the SNMP Manager.



SNMP Messages:

- SNMP Messages are used to communicate between the SNMP Manager and Agents.
- SNMPv1 supports five basic SNMP messages Get, Get-Next, Get-Response, Set & Trap.
- SNMPv2c, two new messages were added Inform and Getbulk.
- GET Messages are sent by the SNMP Manager to retrieve info from SNMP Agents.
- SET Messages are used by the SNMP Manager to assign the value to SNMP Agents.
- GET-NEXT retrieves the value of the next object in the MIB.
- GET-RESPONSE Message is used by SNMP Agents to reply to GET & GET-NEXT messages.
- TRAP Messages are initiated from the SNMP Agents to inform the SNMP Manager on event.
- Inform Message, SNMP Manager acknowledge that the message has been received.
- Getbulk operation efficiently retrieve large blocks of data, such as multiple rows in a table.





SNMPv1:

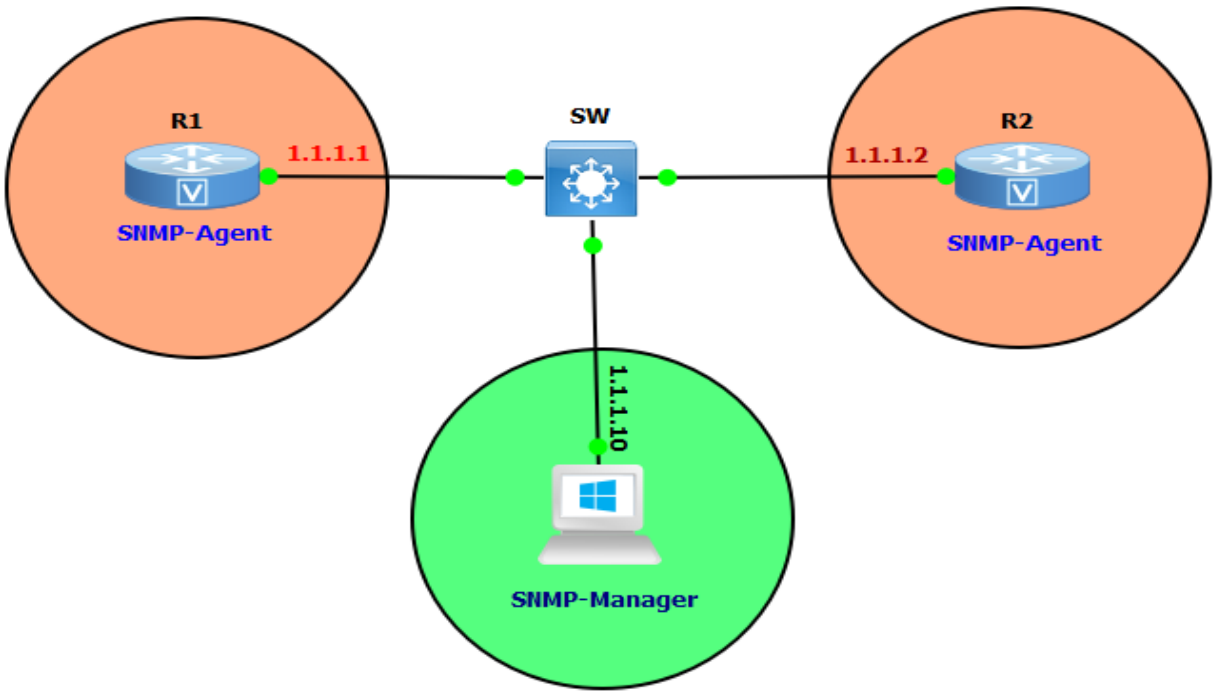
- SNMP version 1 security is based on community strings.
- An SNMP community string can be considered as password.

SNMPv2c:

- SNMPv2c is an update SNMPv2 and SNMPv2c.
- SNMPv2c uses the community-based security model of SNMPv1.
- SNMPv2c "c" in SNMPv2c stands for "community".
- SMMPv2c sends the community strings in clear text.

SNMPv3:

- SNMPv3 is the most secure version among other SNMP versions.
- SNMPv3 provides secure access to devices using authentication & encryption.
- Authentication security feature makes sure that the message is from a valid source.
- Integrity security feature makes sure that the message has not been tampered.
- Encryption security feature provides confidentiality by encrypting the contents.
- SNMPv3 will never send the user password in the clear text.
- SNMPv3 uses the SHA1 or MD5 hash-based authentication.
- SNMPv3 encryption is done using the AES, 3DES and DES.
- SNMP offers three security levels: noAuthNoPriv, AuthNoPriv and AuthPriv.
- Auth stands for Authentication and Priv for Privacy.
- NoAuthNoPriv = no authentication and no encryption.
- AuthNoPriv = authentication but no encryption.
- AuthPriv = authentication AND encryption.



SNMP V2 Configuration
R1(config)# snmp-server community cisco ro
R1(config)# snmp-server community cisco rw
R1(config)# snmp-server location DC
R1(config)# snmp-server contact admin
R1(config)# snmp-server host 1.1.1.10 version 2c test
R1(config)# snmp-server enable traps
R1# show snmp group
R1# show snmp user
R1# show snmp engine ID

SNMP V3 No Authentication & Privacy
R1(config)# snmp-server group group1 v3 noauth
R1(config)# snmp-server user user1 group1 v3
R1(config)# snmp-server enable traps
R1(config)# snmp-server host 1.1.1.10 user1

SNMPV3 Authentication & Privacy Configuration
R1(config)# snmp-server group group1 v3 auth
R1(config)# snmp-server user user1 group1 v3 auth md5 authpass
R1(config)# snmp-server enable traps
R1(config)# snmp-server host 1.1.1.10 user1
R1# show snmp group
R1# show snmp user
R1# show snmp