

Simple Network Management Protocol (SNMP):

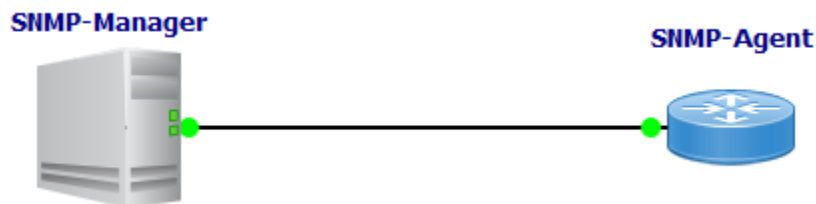
- o SNMP is term which is stands for Simple Network Management Protocol.
- o SNMP is used to monitor and manage devices on your whole networks.
- o It has several uses, from monitoring & generating alerts to device configuration.
- o Simple Network Management Protocol (SNMP) is the application layer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

SNMP Manager:

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

SNMP Agent:

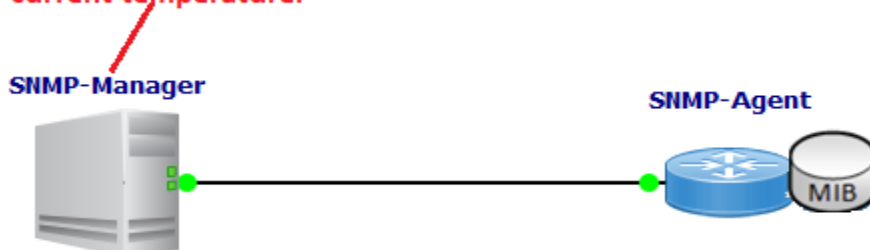
- o A software runs on network devices that we want to monitor router, firewall, etc.



Management Information Base (MIB):

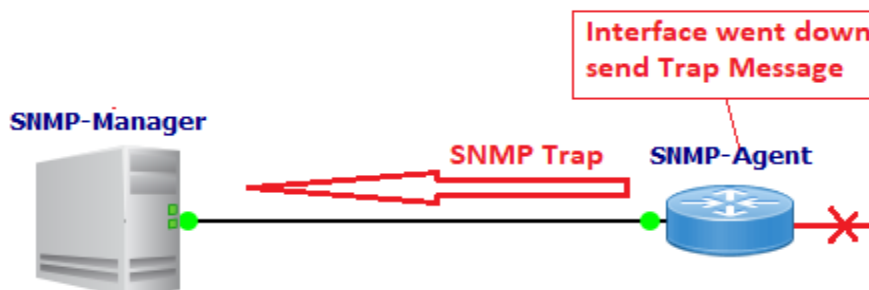
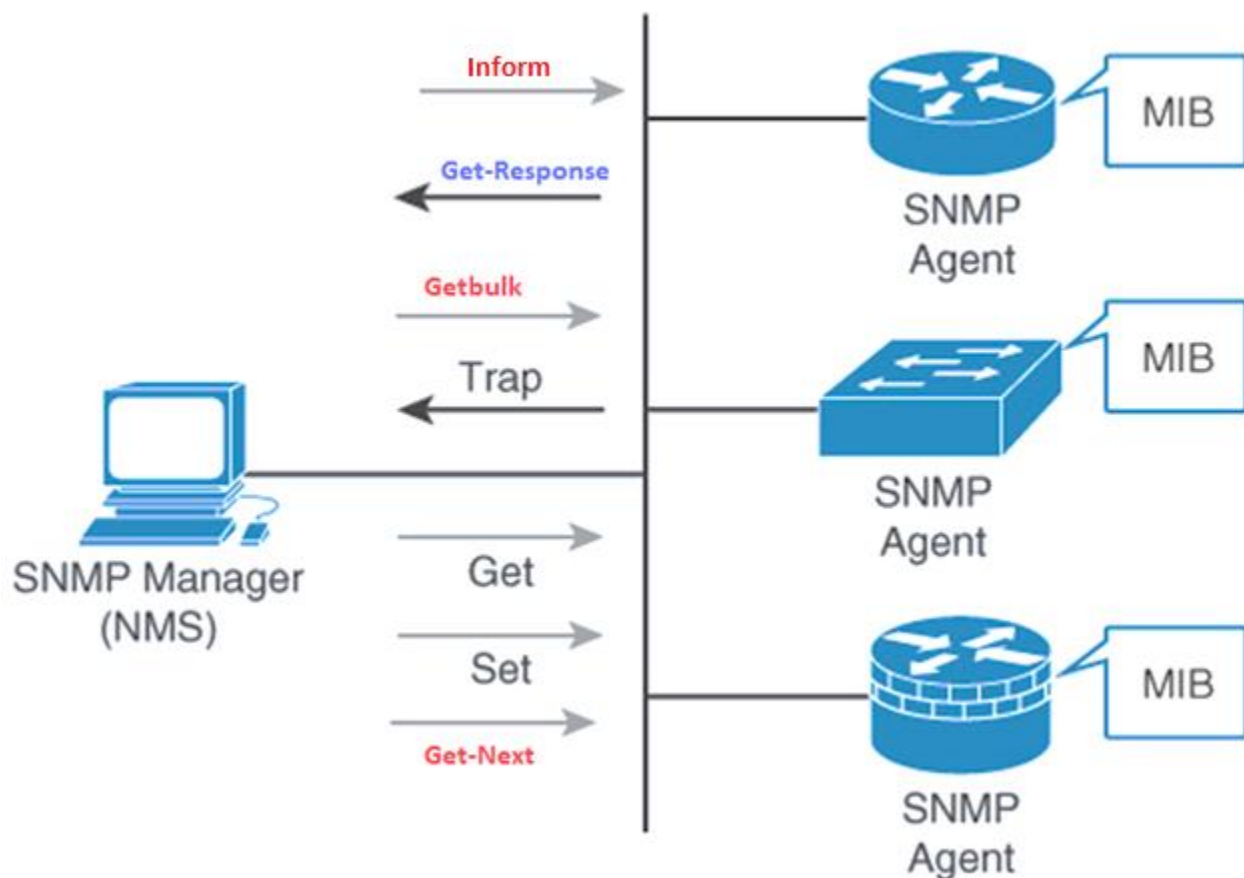
- o Management Information Base (MIB) is the collection of managed objects.
- o MIB contains a set of questions that the SNMP Manager can ask the Agent.
- o MIB contains a set of questions that the Agent can understand them.
- o MIB is commonly shared between the Agent and the SNMP Manager.

Check MIB Variable to discover current temperature.



SNMP Messages:

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



SNMP Version 1:

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

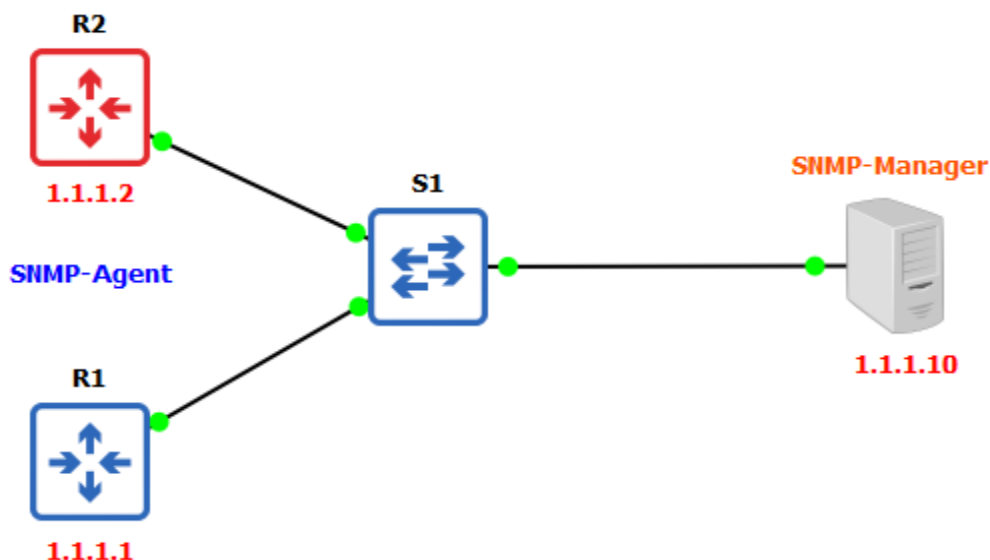
SNMP Version 2c:

- o SNMPv2c is an update SNMPv2 and SNMP Version 1.
- o SNMPv2c uses the community-based security model of SNMPv1.
- o SNMPv2c "c" in SNMPv2c stands for "community".
- o SMMPv2c sends the community strings in clear text.

SNMP Version 3:

- o SNMP Version 3 is the most secure version among other SNMP versions.
- o SNMP V3 provides secure access to devices using authentication & encryption.
- o Authentication security feature makes sure that message is from a valid source.
- o Integrity security feature makes sure that the message has not been tampered.
- o Encryption security feature provides confidentiality by encrypting the contents.
- o SNMP Version 3 will never send the user and the password in the clear text.
- o SNMP Version 3 uses the SHA1 or the MD5 hash-based authentication methods.
- o SNMP Version 3 encryption is done using the methods AES, 3DES and the DES.
- o SNMP offers three security levels: noAuthNoPriv, AuthNoPriv and AuthPriv.
- o Auth stands for Authentication and Priv stand for Privacy in SNMP Version 3.
- o **NoAuthNoPriv** = no authentication & no encryption of the messages send & receive.
- o **AuthNoPriv** = authentication but no encryption of the messages send and receive.
- o **AuthPriv** = authentication necessary and messages are encrypted send and receive.

Lab Time:



Devices Basic Configuration

```
R1(config)#interface ethernet 0/0  
R1(config-if)#ip address 1.1.1.1 255.0.0.0  
R1(config-if)#no shutdown
```

```
R2(config)#interface ethernet 0/0  
R2(config-if)#ip address 1.1.1.2 255.0.0.0  
R2(config-if)#no shutdown
```

```
S1(config)#interface vlan 1  
S1(config-if)#ip address 1.1.1.3 255.0.0.0  
S1(config-if)#no shutdown
```

SNMP Version 2 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 Version 3 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
```

SNMP Version 3 Authentication & No Privacy Configuration

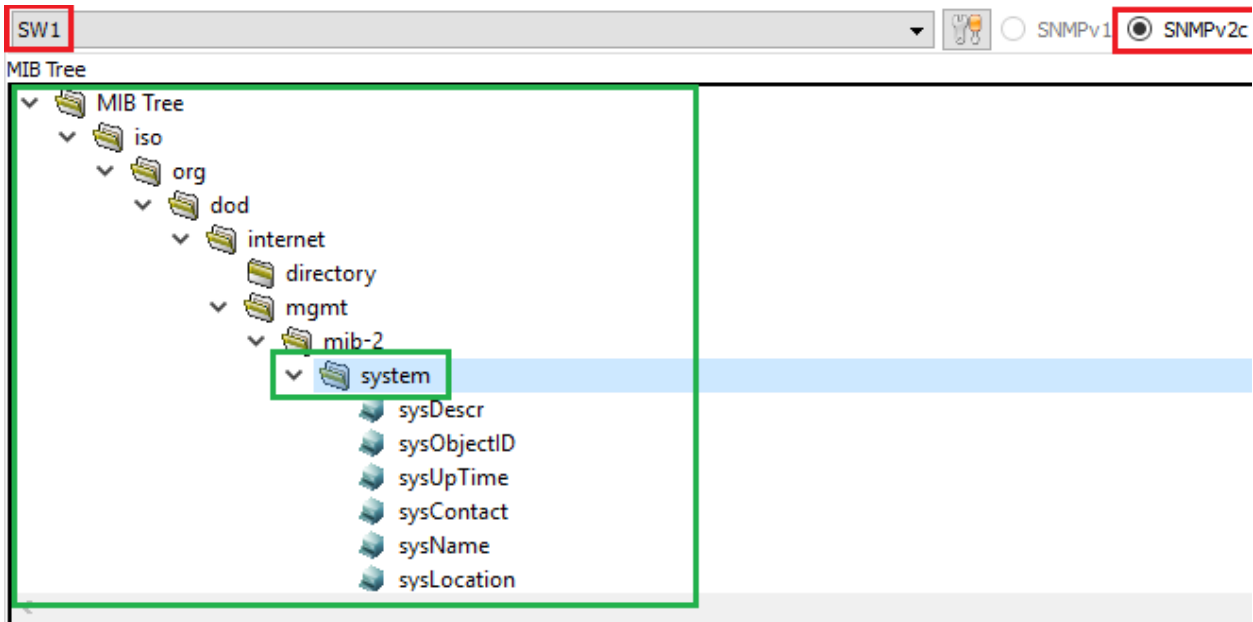
```
R1(config)# snmp-server group group1 v3 auth  
R1(config)# snmp-server user user1 group1 v3 auth md5 authpass  
R1(config)# snmp-server enable traps  
R1(config)# snmp-server host 1.1.1.10 user1
```

SNMP Version 3 Authentication & Privacy Configuration

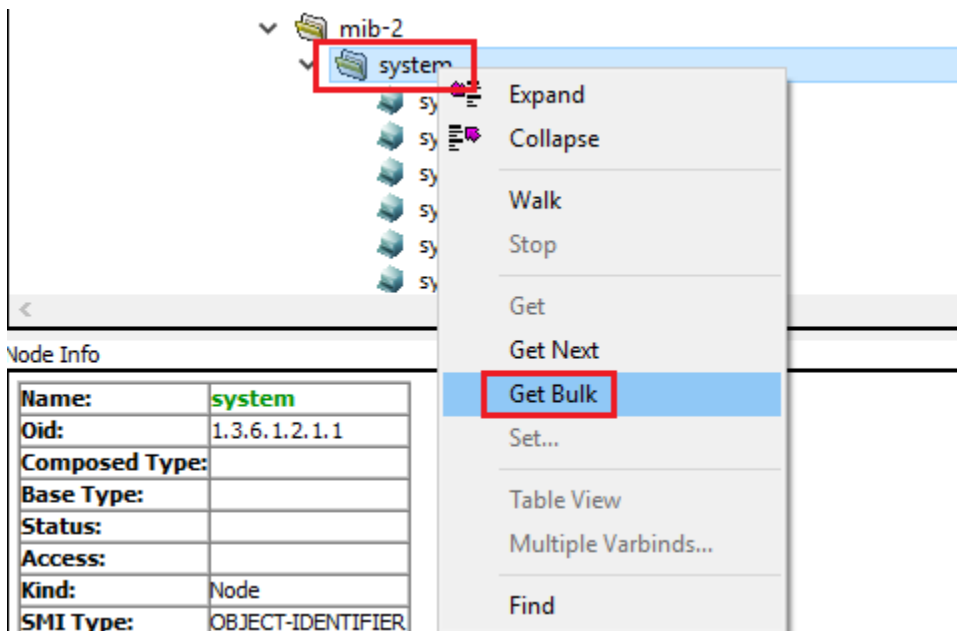
```
R1(config)# snmp-server group group1 v3 auth  
R1(config)# snmp-server user user1 group1 v3 auth md5 authpass  
R1(config)# snmp-server enable traps  
R1(config)# snmp-server host 1.1.1.10 user1  
R1# show snmp group  
R1# show snmp user  
R1# show snmp
```

SNMP Messages:

Get, Get-Next, Get-Response, Set and Getbulk.



Getbulk operation efficiently retrieve large blocks of data, such as multiple rows in a table.



Getbulk operation efficiently retrieve large blocks of data, System Description, System UP Time, System Contact, and System name, System Location, System Services etc.

```
Query Results
-----SNMP query started-----
1: sysDescr.0 Cisco IOS Software, Linux Software (I86BI_LINUXL2-IPBASEK9-M), Experimental Version 15.
2: sysObjectID.0 enterprises.9.1.1227
3: sysUpTime.0 1:33:59.76
4: sysContact.0 admin
5: sysName.0 SW1
6: sysLocation.0 DC
7: sysServices.0 6
8: sysORLastChange.0 0:00:00.00
9: sysORID.1 enterprises.9.7.129
10: sysORID.2 enterprises.9.7.115
-----SNMP query finished-----
Total # of Requests = 1
Total # of Objects = 10
```

GET Messages are sent by the SNMP Manager to retrieve info from SNMP Agents.

The screenshot shows a network management interface. On the left, a tree view under 'system' lists objects: sysDescr, sysObjectID, sysUpTime, sysContact, sysName, and sysLocation. The 'sysName' object is selected, and a context menu is open over it with the 'Get' option highlighted. Below the tree is a 'Node Info' table for 'sysName':

Name:	sysName
Oid:	1.3.6.1.2.1.1.5
Composed Type:	DisplayString
Base Type:	OCTET STRING
Status:	current
Access:	read-write
Kind:	Scalar
SMI Type:	OBJECT-TYPE
Size:	0 .. 255
Module:	SNMPv2-MIB
Description:	An administratively-assigned node. By convention, this is the domain name. If the name is the zero-length string.

On the right, a 'Query Results' window shows the output of the GET request:

```
Query Results
-----SNMP query started-----
1: sysName.0 SW1
-----SNMP query finished-----
Total # of Requests = 1
Total # of Objects = 1
```

SET Messages are used by the SNMP Manager to assign the value to SNMP Agents.

The screenshot illustrates the configuration of the `sysName` variable in an SNMP Manager. On the left, a tree view shows the `system` node expanded, with `sysName` selected. Below the tree is a table of object information:

Object Info	
Name:	sysName
Oid:	1.3.6.1.2.1.1.5
Composed Type:	DisplayString
Base Type:	OCTET STRING
Status:	current
Access:	read-write
Kind:	Scalar
SMI Type:	OBJECT-TYPE

A context menu is open over `sysName`, with the `Set...` option highlighted. On the right, the `Set` dialog box is displayed. It shows the OID `1.3.6.1.2.1.1.5` and a MIB tree view where `sysName` is selected. The `Syntax` is `Octet String`, and the `Value` field is empty. The `Range` is `0 .. 255`. The `OK` button is highlighted.