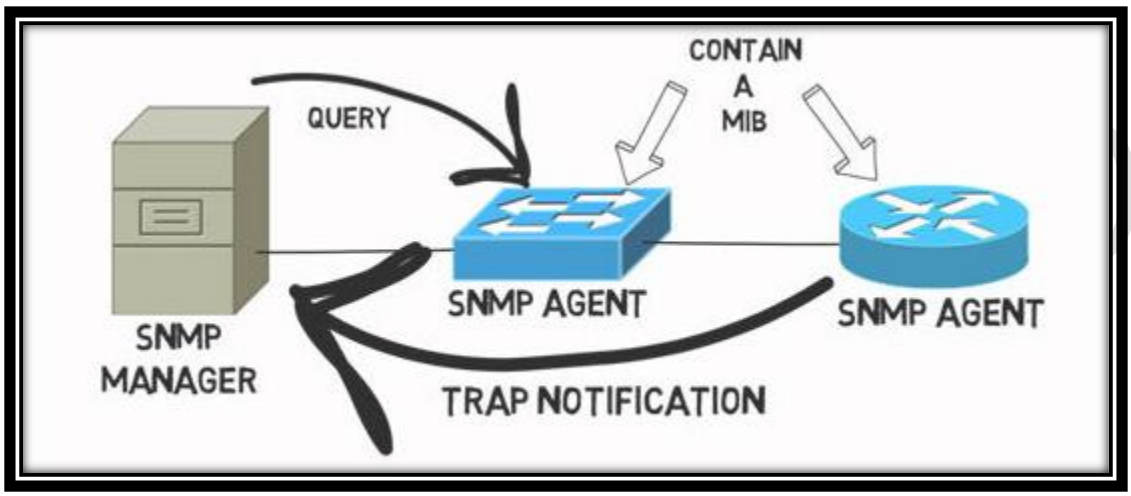

Networkforyou
Welcome
To
Network for you
SNMP
Networkforyou

SNMP (Simple Network Management Protocol):

- SNMP Stand for Simple Network Management Protocol.
- It is Monitoring Protocol.
- It is application Protocol that is used for network management.
- It is used to monitor and manage devices on your whole networks.
- With the help of SNMP Protocol we can retrieve information from network devices.
- And also we can configure network devices with SNMP.
- We have read only and Read write mode with this we can retrieve only information from device and retrieve or configure the network devices respectively.
- All SNMP Message 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 Manger:

- SNMP Manager is the software that is running on a pc or server that will monitor the network devises.

SNMP Agent:

- SNMP Agent runs on the network device like routers, Switches, Server etc.

SNMP Monitoring Tools Example:

- Solar Winds Network Performance Monitor
- Manage Engine OP Manager
- Paessler PRTG Network Monitor
- MRTG

Management Information Base (MIB):

- It is collection of Managed objects
- It contain set of question that the SNMP Manager can ask the Agent
- It commonly shared between the Agent and SNMP Manager.

SNMP Messages:

- SNMP Manager and Agents used SNMP Messages to communicate between them.
- GET Message are sent by the SNMP Manger to retrieve information from SNMP Agents
- SET Message are used by SNMP Manger to assign the value to SNMP Agents.
- GET-NEXT retrieves the value of the next object present in MIB.
- GET-Response Message is used by SNMP Agents to reply to GET and GET-Next messages.
- TRAP Messages are initiated from the SNMP Agents to inform the SNMP Manager on event.
- GETbulk operation efficiently retrieves large blocks of data, such as multiple rows in a table.
- Inform Message is used by SNMP Manager to acknowledge that the message has been received.

We have SNMP Version:

- SNMP Version1 ---------- Limited
- SNMP Version2 ---------- Limited Authentication
- SNMP Version3 ------Increase Security (Encryption)

SNMPv1:

- SNMP version 1 uses **plain text authentication** between the manager and agent using matching community strings.
- SNMP version 1 security is based on community strings.
- An SNMP community string can be considered as password.

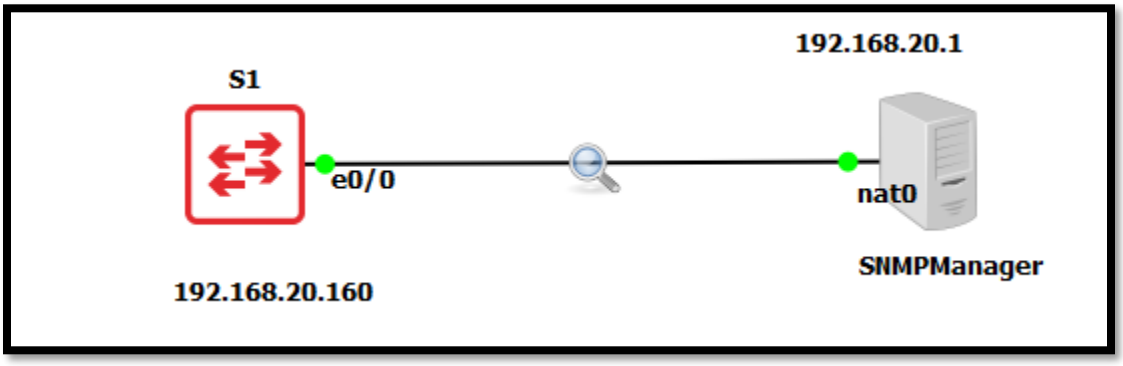
SNMPv2c:

- SNMPv2c is an update SNMPv2.
- SNMPv2c also uses plain text community strings.
- It supports bulk retrieval.

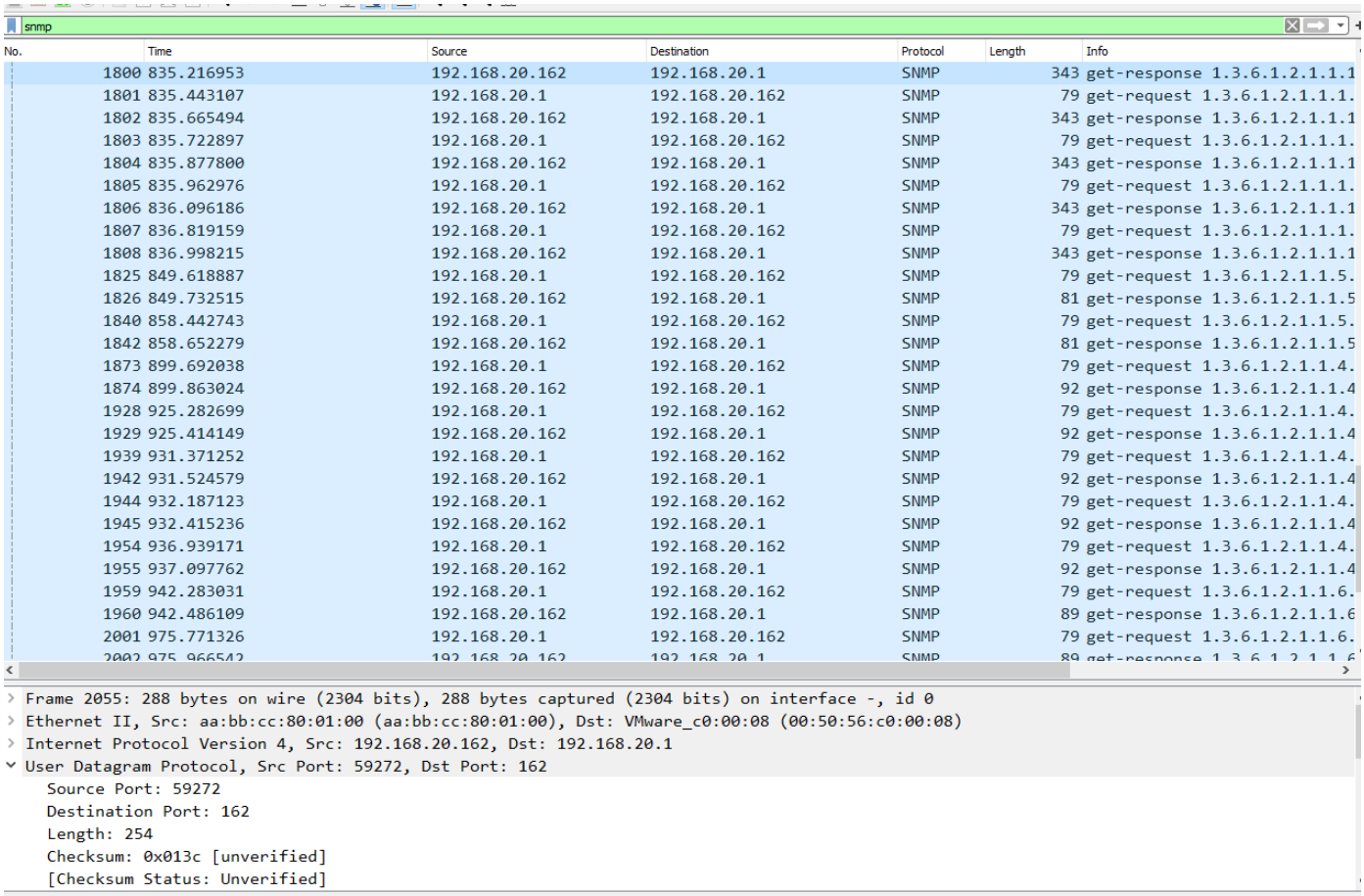
SNMPv3:

- SNMPv3 is the most secure version among other SNMP versions.
- SNMPv3 provides secure access to devices using authentication & encryption.
- SNMPv3 supports strong authentication and encryption. It is the preferred version but it not supported on all devices.
- 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.
- 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.

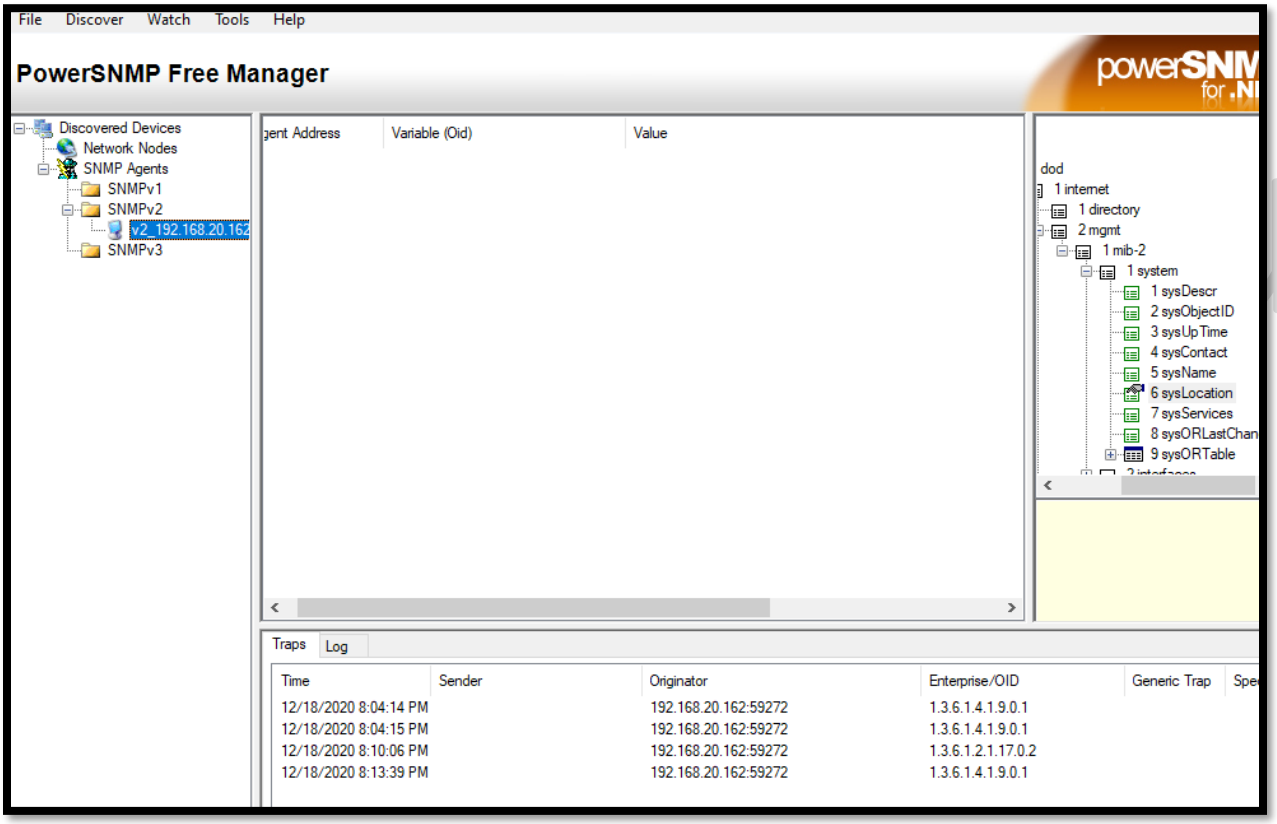
Lab Time:

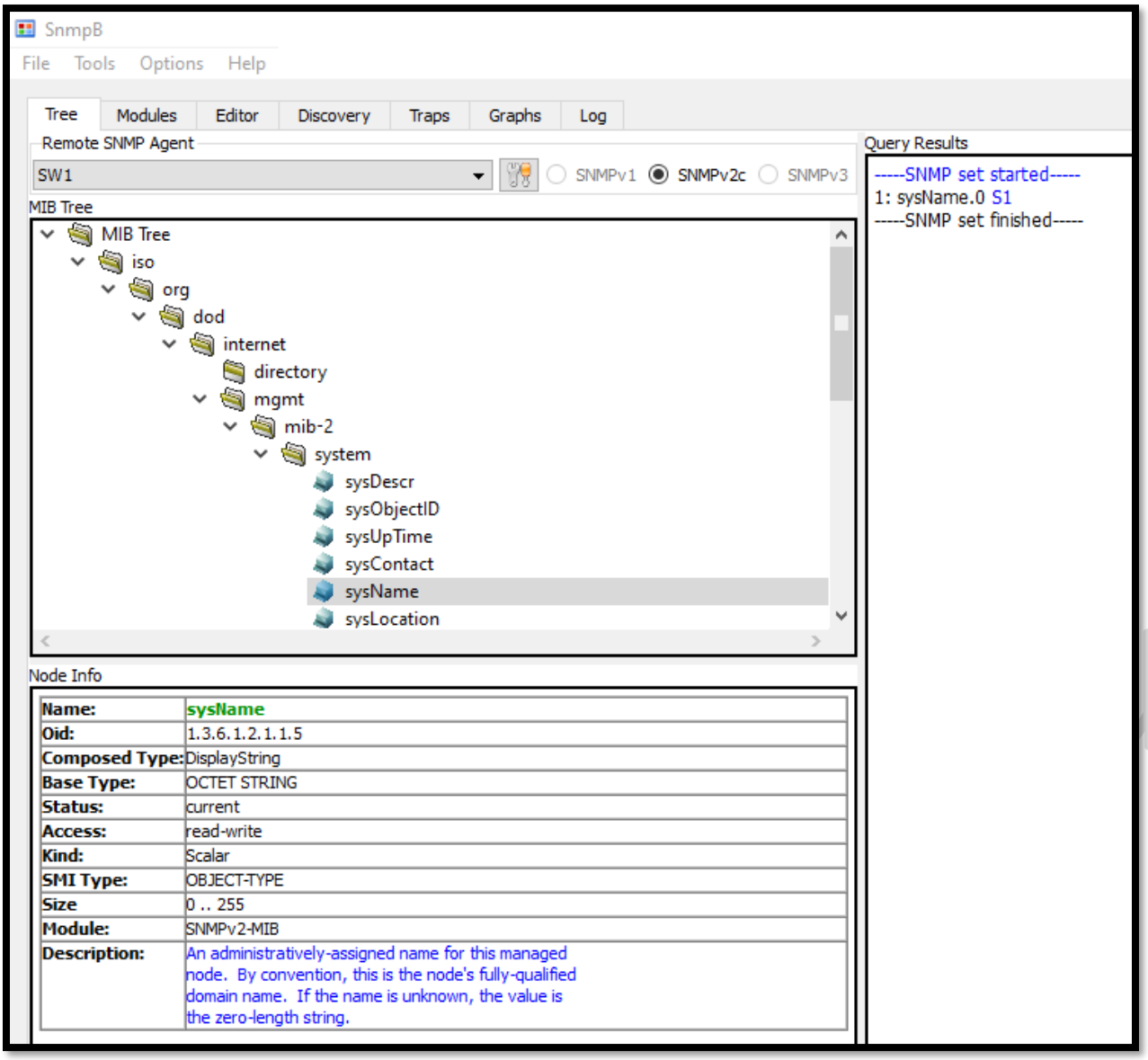


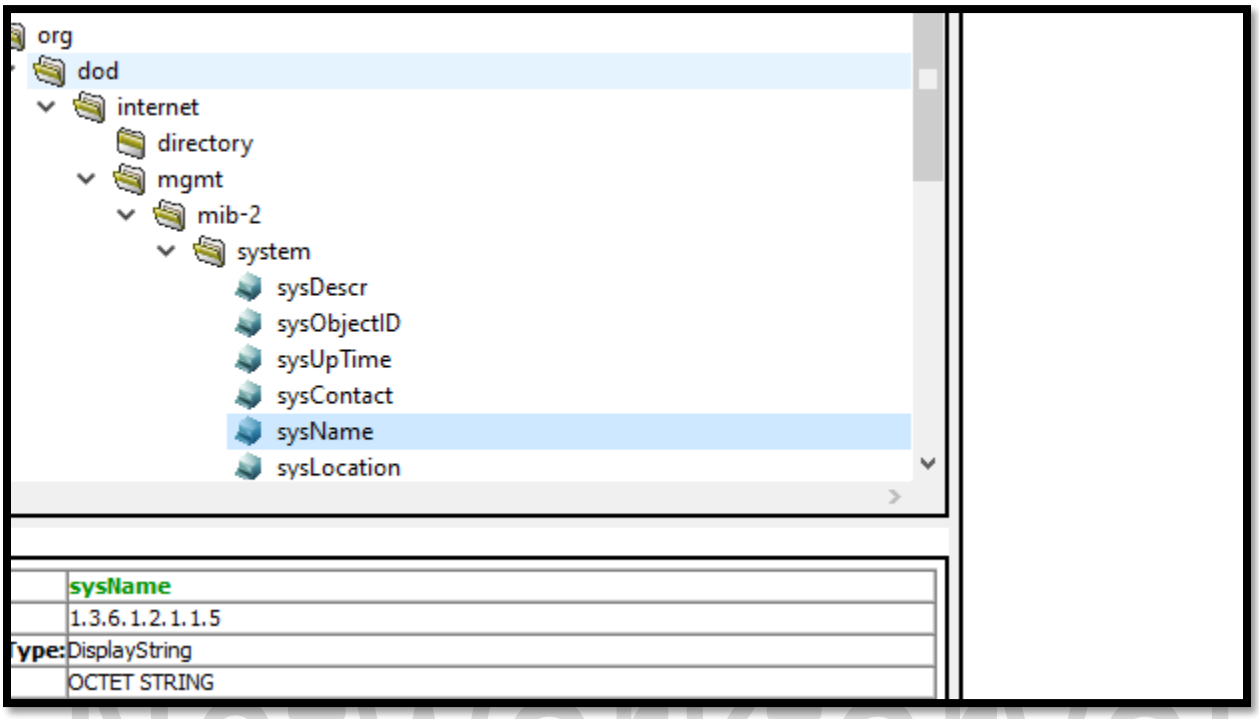
SW1 Basic Configuration:	SNMP V2 Configuration:
en Configuration hostname SW1 int vlan 1 ip add 192.168.20.162 255.255.255.0 no sh	snmp-server community abc snmp-server community abc rw snmp-server location DataCenter snmp-server contact Networkforyou snmp-server host 192.168.38.1 version 2c abc snmp-server enable traps show snmp group show snmp user show snmp engine ID



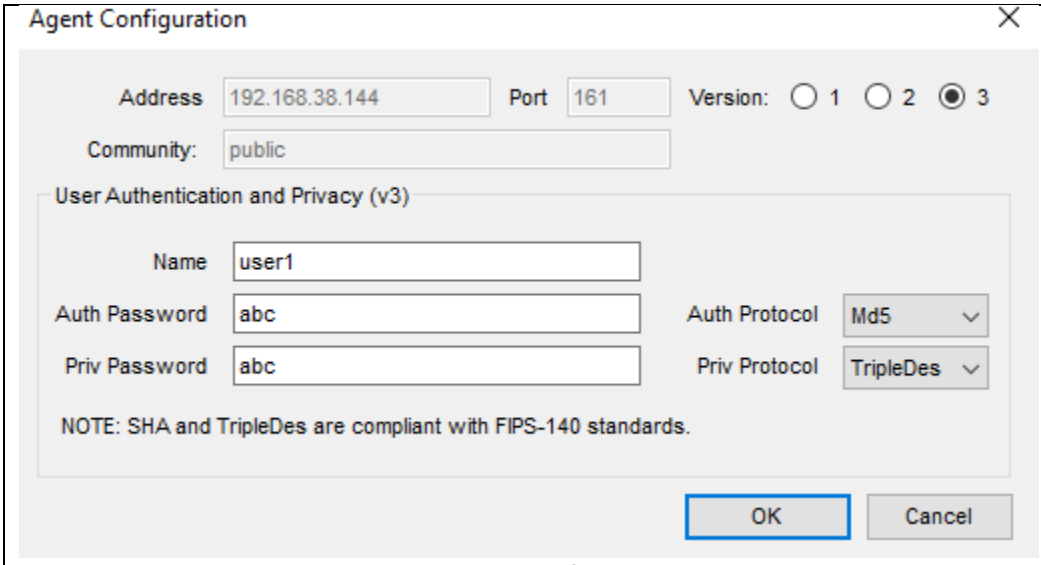
```
    [Stream index: 121]
  > [Timestamps]
Simple Network Management Protocol
    version: v2c (1)
    community: abc
  v data: snmpV2-trap (7)
    v snmpV2-trap
        request-id: 8
        error-status: noError (0)
```




SnmpB
File Tools Options Help
Tree Modules Editor Discovery Traps Graphs Log
Remote SNMP Agent
SW1
SNMPv1 SNMPv2c SNMPv3
MIB Tree
MIB Tree
iso
org
dod
internet
directory
mgmt
mib-2
system
sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLocation
Query Results
-----SNMP set started-----
1: sysName.0 S1
-----SNMP set finished-----
Node 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
Size 0 .. 255
Module: SNMPv2-MIB
Description: An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.



SNMP Version 3 No Authentication & Privacy
snmp-server group group1 v3 noauth snmp-server user user1 group1 v3 snmp-server enable traps snmp-server host 192.168.38.1 user1
SNMP Version 3 Authentication & No Privacy
snmp-server group group1 v3 auth snmp-server user user1 group1 v3 auth md5 abc snmp-server enable traps snmp-server host 192.168.38.1 user1
SNMP Version 3 Authentication & Privacy Configuration
snmp-server group group1 v3 auth snmp-server user user1 group1 v3 auth md5 abc priv 3des abc snmp-server enable traps snmp-server host 192.168.38.1 user1



SNMP Version 3 Authentication & Privacy Configuration

SNMP Troubleshooting:

- SNMP protocol helps network admins to manage, monitor state of network devices.
- Need to be able to ping server from the agent, Layer 3 connectivity is exist or not.
- Ensure that community strings match and the ACLs classifying servers are correct.
- Ensure that configurations for notifications are correct, and that traps are enabled.
- Ensure that host (NMS) IP address, SNMP version & community string are all correct.
- If do not want all traps to be sent, you must specify the correct ones to send to server.
- Check using the correct hashing and the encrypting algorithms, and correct passwords.
- Verify that the community string or the SNMP user is properly configured on the system.
- Verify devices are able to accept SNMP requests from "ALL" sources rather than specific.
- Check that there an ACL in the path between the client and the device blocking port 161.
- Check that there an ACL in the path between the client and the device blocking port 162.

SNMP (Simple Network Management Protocol) is a widely used protocol for monitoring and managing network devices. It is a lightweight protocol that uses UDP port 161 for communication between devices.

There are a number of common SNMP troubleshooting issues that can occur. Some of the most common issues include:

- **Connectivity issues**. SNMP requires that the device and the SNMP manager be able to communicate with each other. If there is a connectivity issue, such as a firewall blocking traffic, SNMP will not be able to function.
- **Configuration issues**. The SNMP agent on the device must be configured correctly in order to receive SNMP requests. If the agent is not configured correctly, SNMP will not be able to communicate with the device.
- **Security issues**. SNMP can be configured to use security features, such as authentication and encryption. If these features are not configured correctly, SNMP can be vulnerable to security attacks.

To troubleshoot SNMP issues, it is important to first identify the specific issue. Once the issue has been identified, there are a number of steps that can be taken to resolve the issue. Some of the most common steps for troubleshooting SNMP issues include:

- **Check connectivity**. The first step is to check connectivity between the device and the SNMP manager. This can be done by using a ping command to verify that the devices can communicate with each other.
- **Check configuration**. The next step is to check the configuration of the SNMP agent on the device. This can be done by reviewing the device documentation or by using the SNMP manager to poll the device for its configuration.
- **Check security**. If the SNMP agent is configured to use security features, it is important to check that these features are configured correctly. This can be done by reviewing the device documentation or by using the SNMP manager to poll the device for its security configuration.

If the above steps do not resolve the SNMP issue, it may be necessary to contact the device manufacturer for assistance.