



Networkforyou

Subscribe to our
You Tube Channel



Networkforyou



**Welcome
To
Network for you
SNMP**



Email us:
networkforyou4@gmail.com

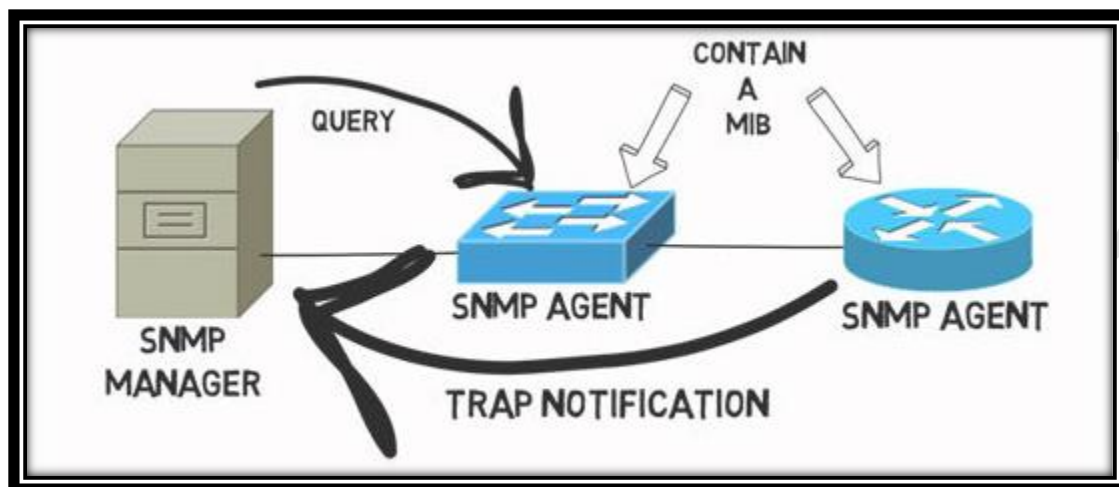
1 of 10

WhatsApp Us : +918143809578



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.

Email us:
networkforYou4@gmail.com

2 of 10

WhatsApp Us : +918143809578



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.

Email us:
networkforYou4@gmail.com

3 of 10

WhatsApp Us : +918143809578



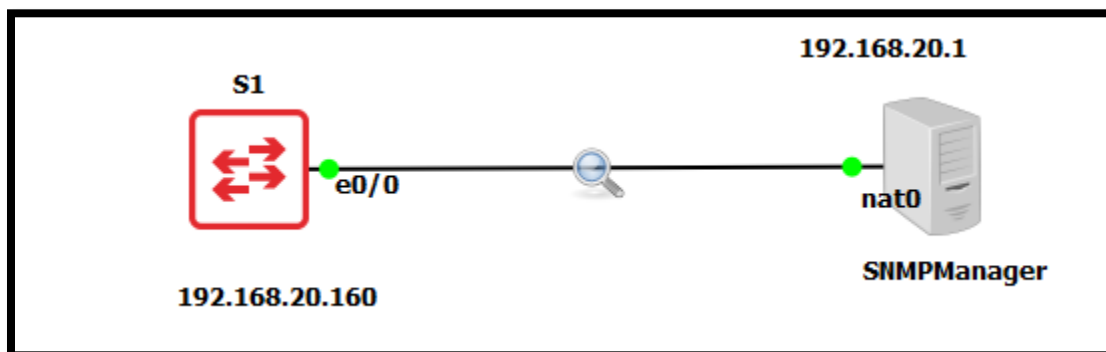
SNMPv2c:

- 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:



Email us:
networkforyou4@gmail.com

4 of 10

WhatsApp Us : +918143809578



SW1 Basic Configuration:	SNMP V2 Configuration:
<pre> en Configuration hostname SW1 int vlan 1 ip add 192.168.20.162 255.255.255.0 no sh </pre>	<pre> 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 </pre>

No.	Time	Source	Destination	Protocol	Length	Info
1800	835.216953	192.168.20.162	192.168.20.1	SNMP	343	get-response 1.3.6.1.2.1.1.1
1801	835.443107	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.1
1802	835.665494	192.168.20.162	192.168.20.1	SNMP	343	get-response 1.3.6.1.2.1.1.1
1803	835.722897	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.1
1804	835.877800	192.168.20.162	192.168.20.1	SNMP	343	get-response 1.3.6.1.2.1.1.1
1805	835.962976	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.1
1806	836.096186	192.168.20.162	192.168.20.1	SNMP	343	get-response 1.3.6.1.2.1.1.1
1807	836.819159	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.1
1808	836.998215	192.168.20.162	192.168.20.1	SNMP	343	get-response 1.3.6.1.2.1.1.1
1825	849.618887	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.5
1826	849.732515	192.168.20.162	192.168.20.1	SNMP	81	get-response 1.3.6.1.2.1.1.5
1840	858.442743	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.5
1842	858.652279	192.168.20.162	192.168.20.1	SNMP	81	get-response 1.3.6.1.2.1.1.5
1873	899.692038	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.4
1874	899.863024	192.168.20.162	192.168.20.1	SNMP	92	get-response 1.3.6.1.2.1.1.4
1928	925.282699	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.4
1929	925.414149	192.168.20.162	192.168.20.1	SNMP	92	get-response 1.3.6.1.2.1.1.4
1939	931.371252	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.4
1942	931.524579	192.168.20.162	192.168.20.1	SNMP	92	get-response 1.3.6.1.2.1.1.4
1944	932.187123	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.4
1945	932.415236	192.168.20.162	192.168.20.1	SNMP	92	get-response 1.3.6.1.2.1.1.4
1954	936.939171	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.4
1955	937.097762	192.168.20.162	192.168.20.1	SNMP	92	get-response 1.3.6.1.2.1.1.4
1959	942.283031	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.6
1960	942.486109	192.168.20.162	192.168.20.1	SNMP	89	get-response 1.3.6.1.2.1.1.6
2001	975.771326	192.168.20.1	192.168.20.162	SNMP	79	get-request 1.3.6.1.2.1.1.6
2002	975.966542	192.168.20.162	192.168.20.1	SNMP	89	get-response 1.3.6.1.2.1.1.6

> Frame 2055: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface -, id 0
> Ethernet II, Src: aa:bb:cc:80:01:00 (aa:bb:cc:80:01:00), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
> Internet Protocol Version 4, Src: 192.168.20.162, Dst: 192.168.20.1
v User Datagram Protocol, Src Port: 59272, Dst Port: 162
Source Port: 59272
Destination Port: 162
Length: 254
Checksum: 0x013c [unverified]
[Checksum Status: Unverified]

Email us:
networkforyou4@gmail.com

WhatsApp Us : +918143809578



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

PowerSNMP Free Manager

Discovered Devices

- Network Nodes
- SNMP Agents
 - SNMPv1
 - SNMPv2
 - 192.168.20.162
 - SNMPv3

Agent Address	Variable (OID)	Value

Traps Log

Time	Sender	Originator	Enterprise/OID	Generic Trap	Spe
12/18/2020 8:04:14 PM		192.168.20.162:59272	1.3.6.1.4.1.9.0.1		
12/18/2020 8:04:15 PM		192.168.20.162:59272	1.3.6.1.4.1.9.0.1		
12/18/2020 8:10:06 PM		192.168.20.162:59272	1.3.6.1.2.1.17.0.2		
12/18/2020 8:13:39 PM		192.168.20.162:59272	1.3.6.1.4.1.9.0.1		

Email us:
networkforyou4@gmail.com

WhatsApp Us : +918143809578



The screenshot shows the SnmpB application interface. The 'Remote SNMP Agent' is set to 'SW1'. The 'MIB Tree' is expanded to show the 'system' node under 'mib-2'. The 'Node Info' panel for 'sysName' is displayed below.

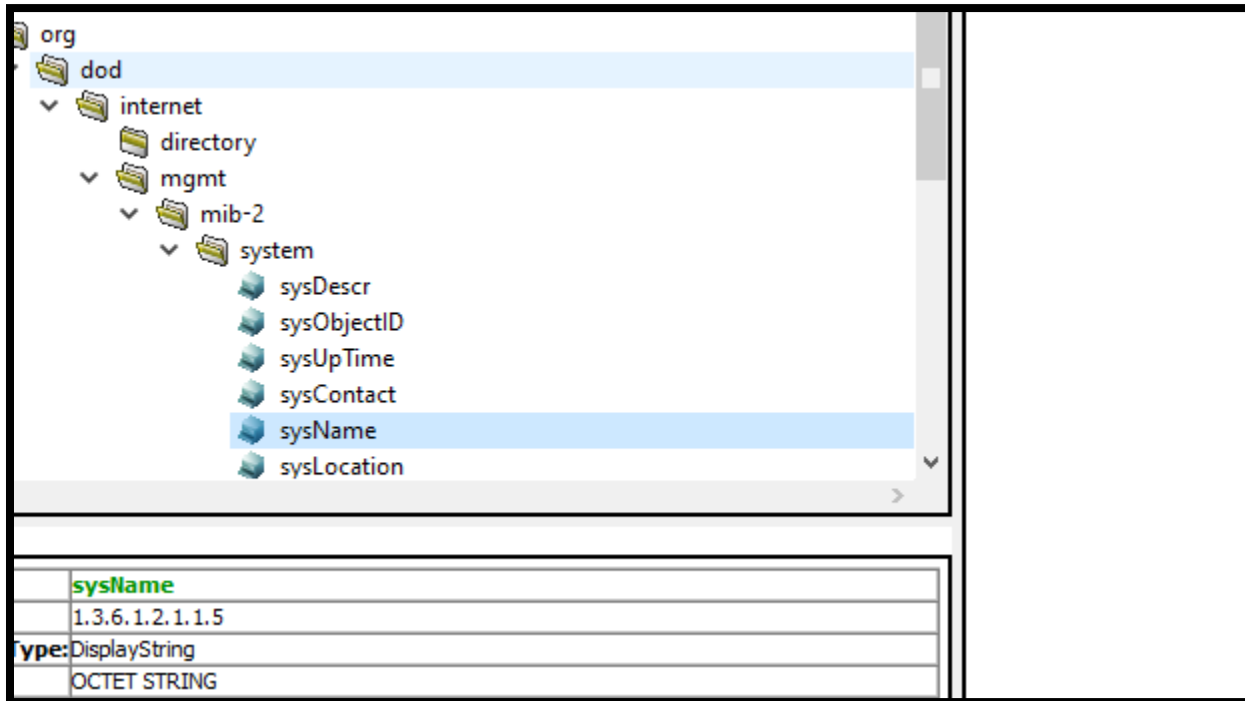
Name:	sysName
Oid:	1.3.6.1.2.1.1.5
Composed Type:	DisplayString
Base Type:	OCTET STRING
Status:	current
Access:	read-write
Kind:	Scalar
SMI Type:	OBJECT-TYPE
Size:	0 .. 255
Module:	SNMPv2-MIB
Description:	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified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

The 'Query Results' panel on the right shows the following output:

```
-----SNMP set started-----  
1: sysName.0 S1  
-----SNMP set finished-----
```

Email us:
networkforyou4@gmail.com

WhatsApp Us : +918143809578



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
```

Email us:
networkforyou4@gmail.com

8 of 10

WhatsApp Us : +918143809578



Agent Configuration

Address: 192.168.38.144 Port: 161 Version: 1 2 3

Community: public

User Authentication and Privacy (v3)

Name: user1

Auth Password: abc Auth Protocol: Md5

Priv Password: abc Priv Protocol: TripleDes

NOTE: SHA and TripleDes are compliant with FIPS-140 standards.

OK Cancel

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.

Email us:
networkforyou4@gmail.com

9 of 10

WhatsApp Us : +918143809578



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.

Email us:
networkforyou4@gmail.com

10 of 10

WhatsApp Us : +918143809578