Lab 6: SNMPv3 Security

NET311 - Computer Network Management

Instructor: Dr. Mostafa Dahshan

Objectives

1. Understanding security features in SNMPv3.
2. Configuring views, groups and users on Cisco routers.
3. Configuring SNMPv3 USM profiles on the SNMP manager.
4. Analyzing SNMPv3 traffic using Wireshark.

References

1. CBT Nuggets, MicroNugget: SNMPv3.
2. GBT Nuggets, MicroNugget: Understanding and Configuring SNMPv3.

Instructions

1. Read the lab instructions.
2. Provide question answers and screenshots in the supplied answer sheet.
3. After finishing the lab, upload your saved answer sheet to LMS.

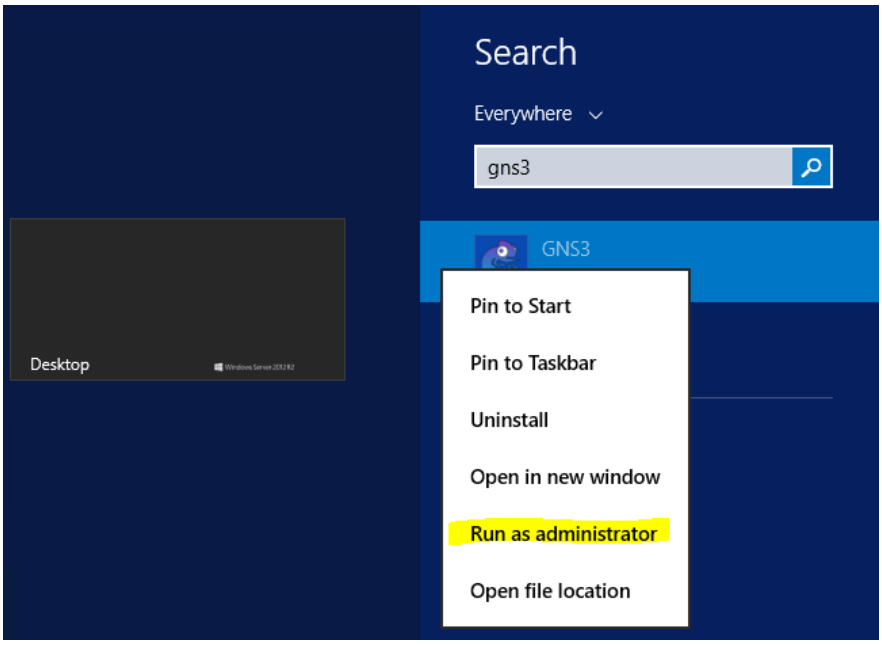
Part 1: Lab Setup

The lab setup required is the same as the lab setup for Lab 05. If you have not performed Lab 05, you must perform Part 1 in Lab 05 before completing this lab.

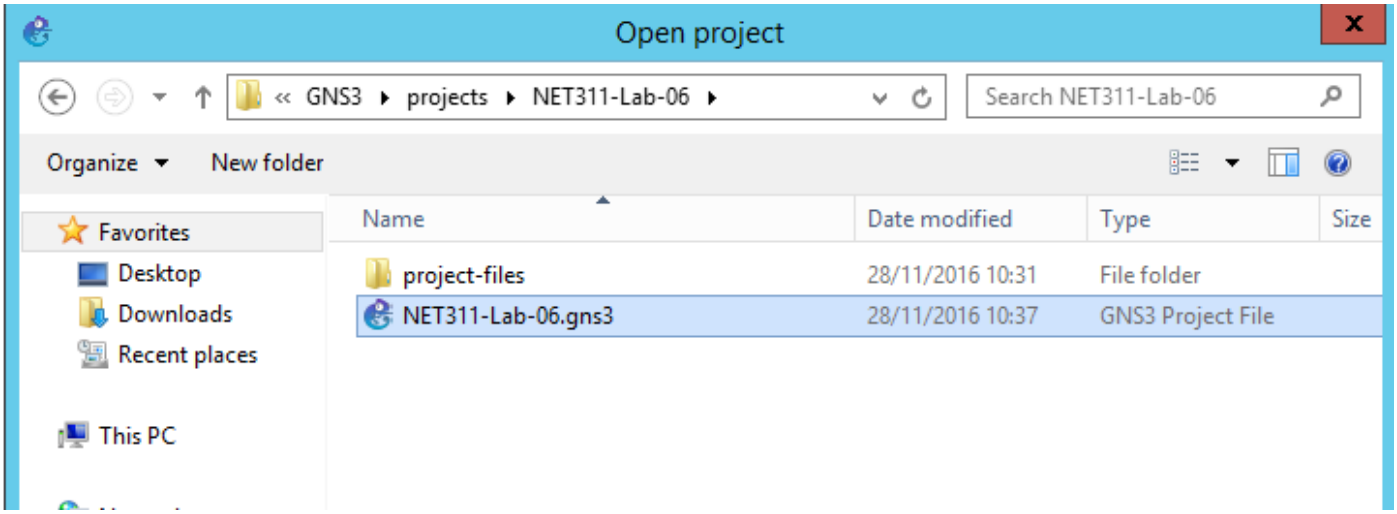
Part 2: SNMPv3 Security configuration on a Cisco router

In this part, we will setup a view called VIEW1 that can access anything below the system OID. Then, we will create a group called GROUP1 and give it access to view VIEW1. Finally, we will create a user called USER1 and add him to GROUP1.

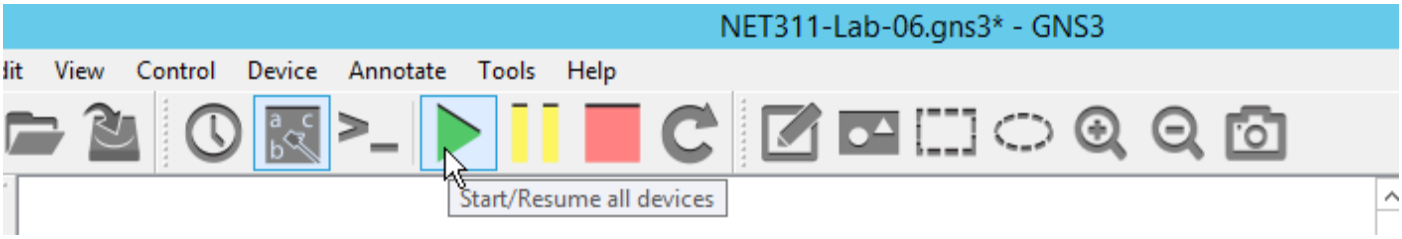
1. Run **GNS3** as an **administrator**.



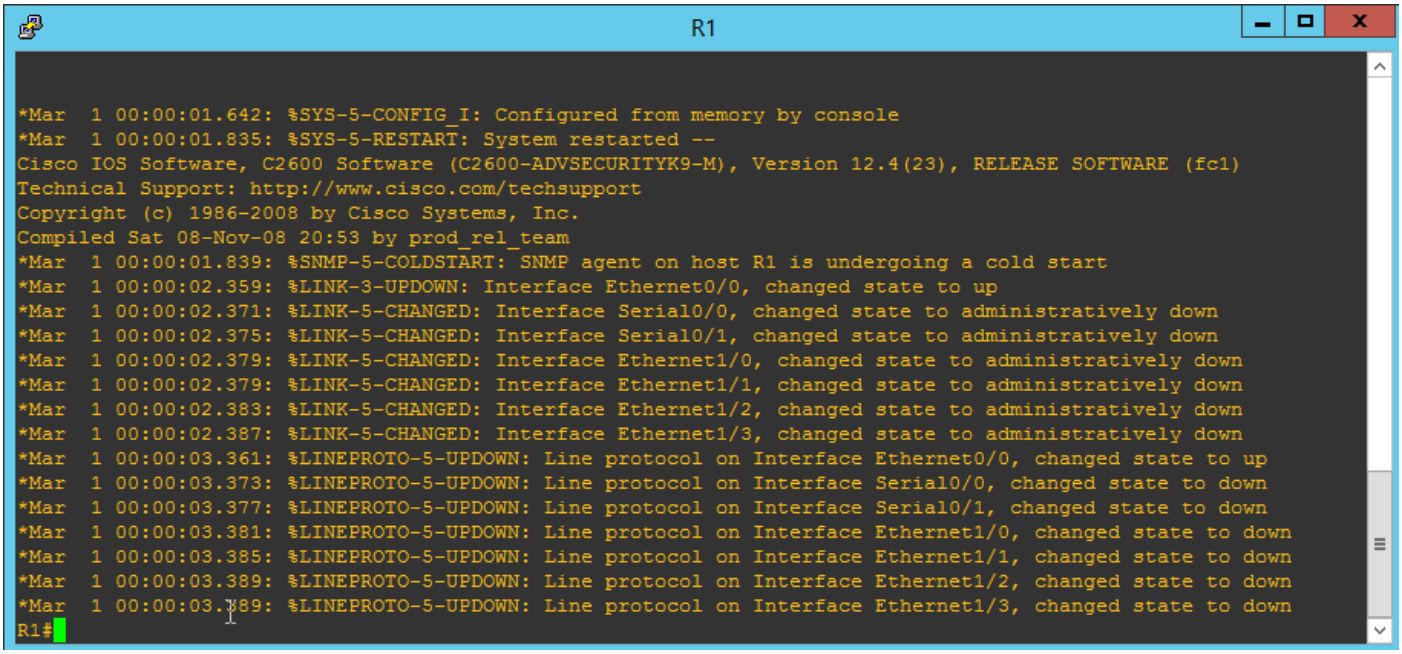
2. Open the GNS3 project **NET311-Lab-06.gns3**.



3. Run the network by clicking on the green icon.



1. After the network is started, double click on the R1 router to access its console.



4. Configure the SNMPv3 engine ID.

```
config t
snmp-server engineID local 123456789A
```

5. Configure SNMPv3 views and groups.

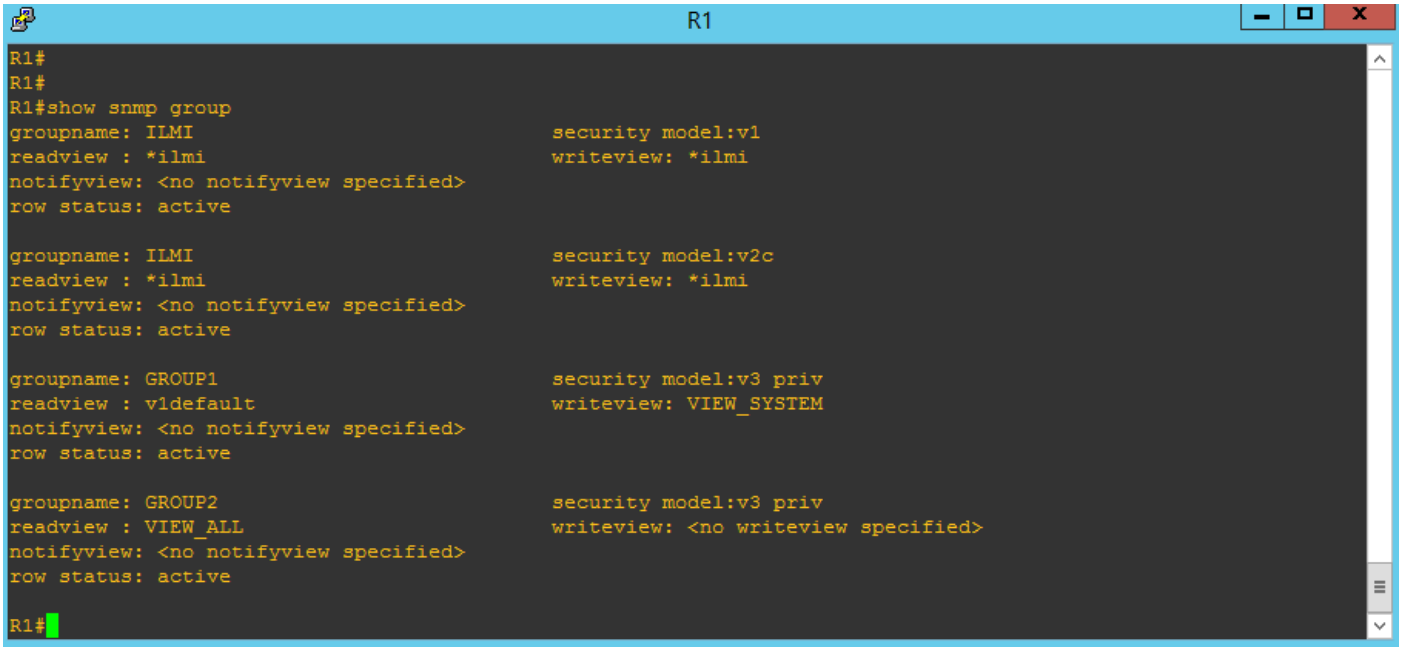
```
snmp-server engineID local 123456789A
snmp-server view VIEW_SYSTEM system included
snmp-server view VIEW_ALL iso included
snmp-server group GROUP1 v3 priv write VIEW_SYSTEM
snmp-server group GROUP2 v3 priv read VIEW_ALL
```

6. Configure SNMPv3 users.

```
snmp-server user USER1 GROUP1 v3 auth sha Auth1 priv des56 Enc1
snmp-server user USER2 GROUP2 v3 auth sha Auth2 priv des56 Enc2
end
```

7. Verify the groups you have created by typing the following command:

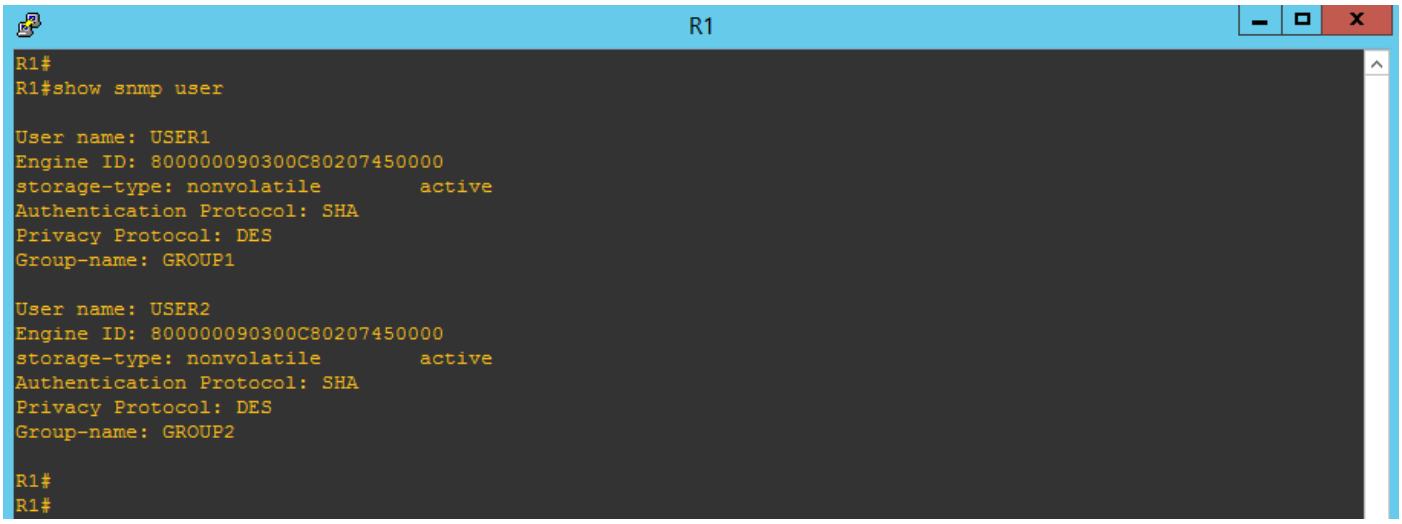
```
show snmp group
```



Lab sheet 2.1: provide a screenshot of the result of the show snmp group command.

8. Verify the users you have created by typing the following command:

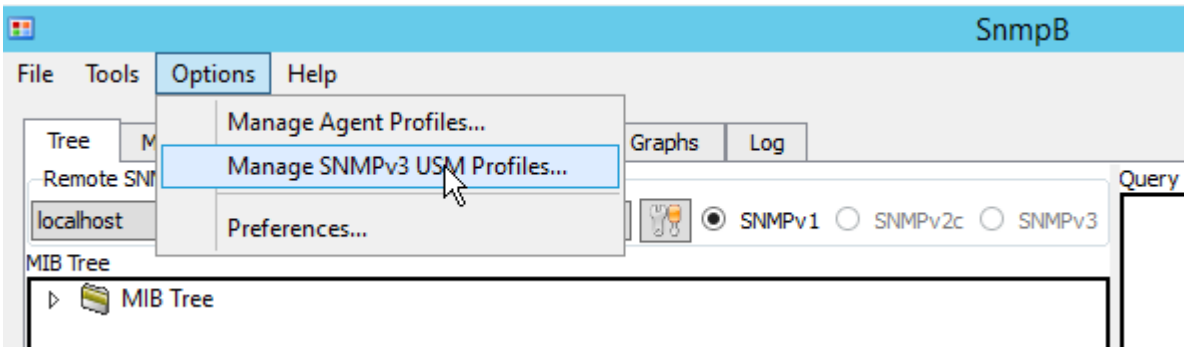
```
show snmp user
```



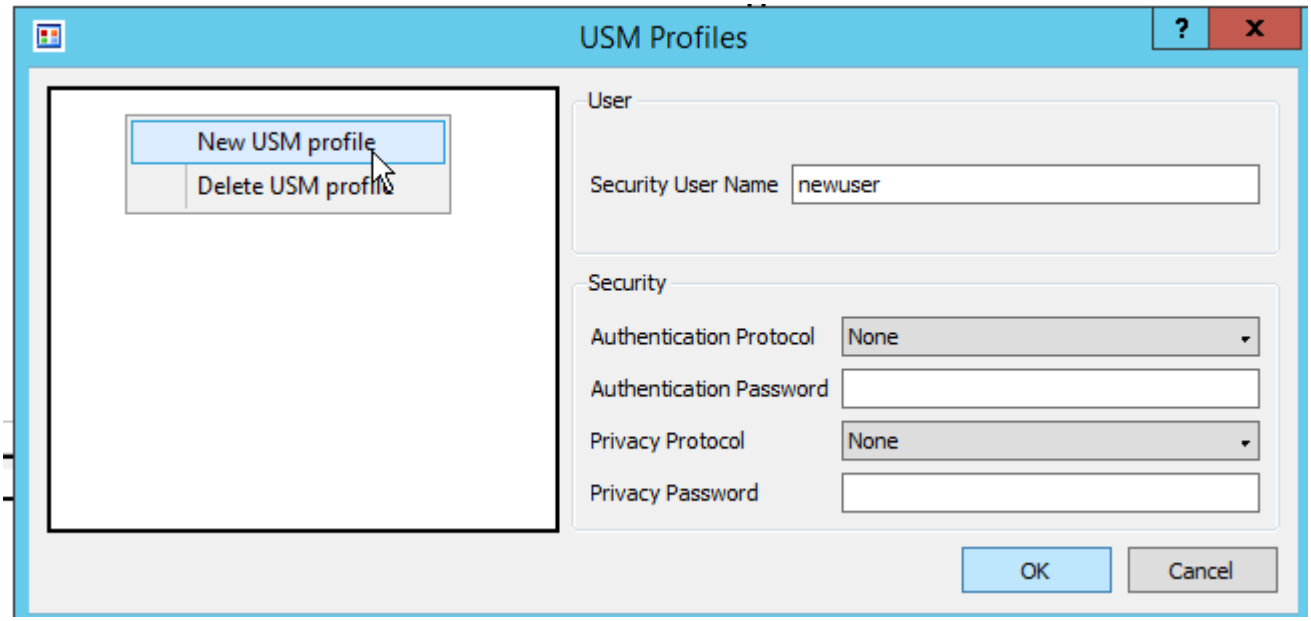
Lab sheet 2.2: provide a screenshot of the result of the show snmp user command.

Part 3: SNMPv3 USM Configuration on the SNMP manager

1. Run SnmpB, then click on Options -> Manage SNMPv3 USM Profiles.



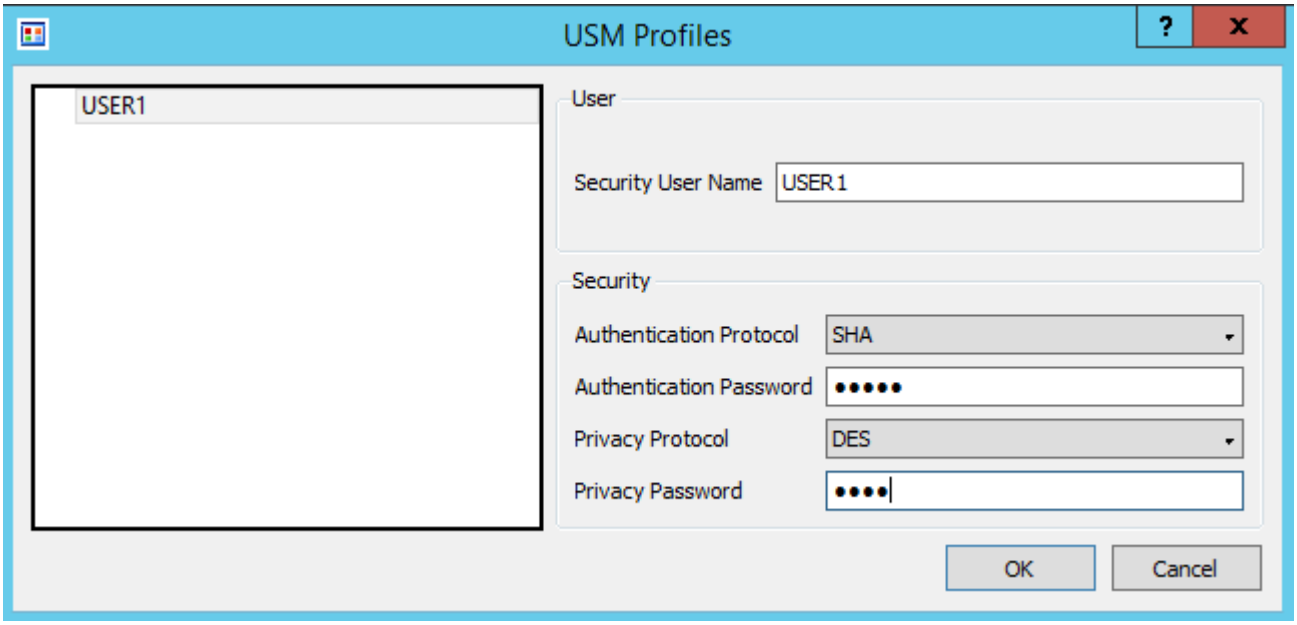
2. Right click and select New USM profile



3. Create a profile for user **USER1** with the following settings:

Select **SHA** for Authentication Protocol and **DES** for Privacy Protocol.

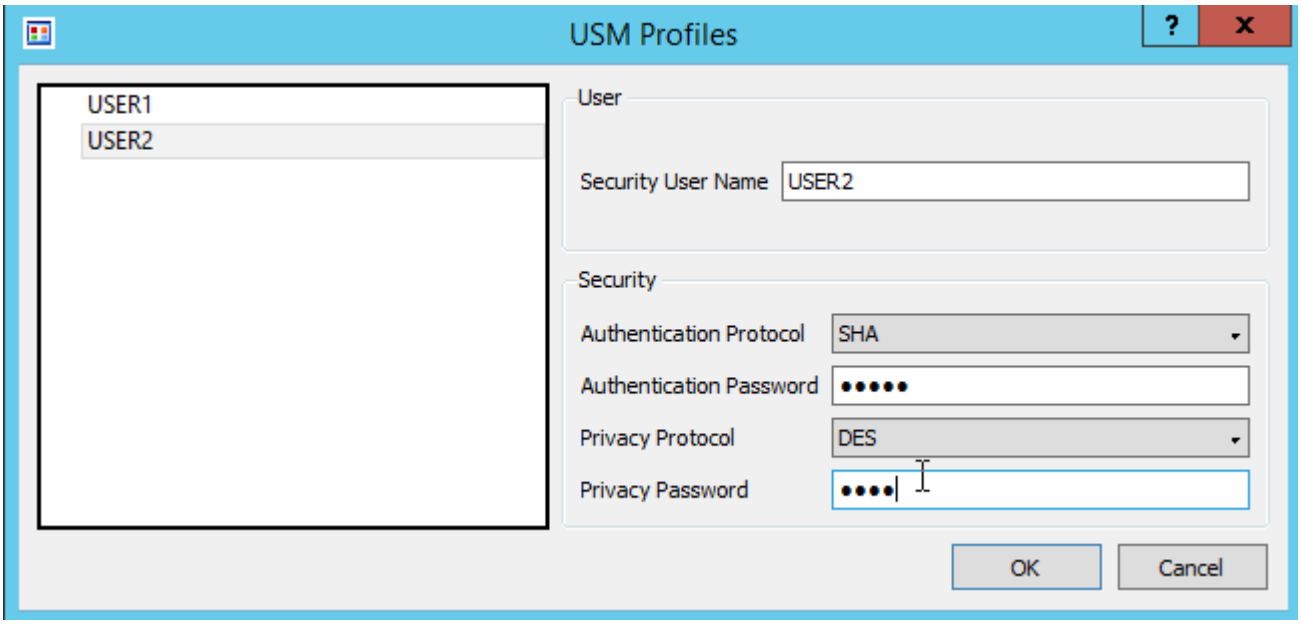
Authentication password is **Auth1** and Privacy password is **Enc1**.



4. Create a profile for user **USER2** with the following settings:

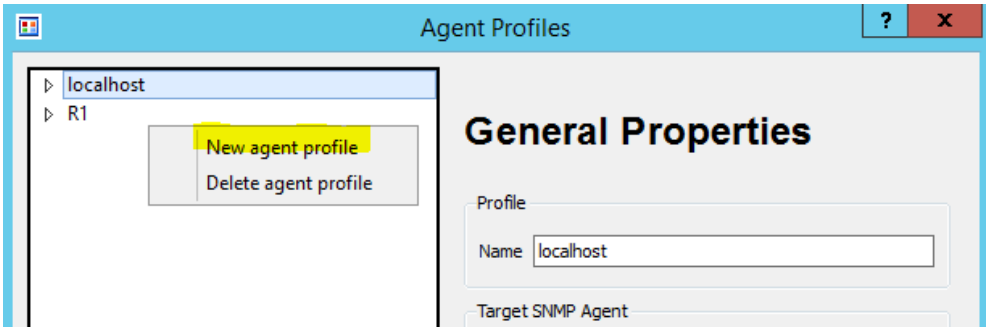
Select **SHA** for Authentication Protocol and **DES** for Privacy Protocol.

Authentication password is **Auth2** and Privacy password is **Enc2**.



Lab sheet 3.1: provide a screenshot showing USM Profiles.

5. Create a new agent profile.

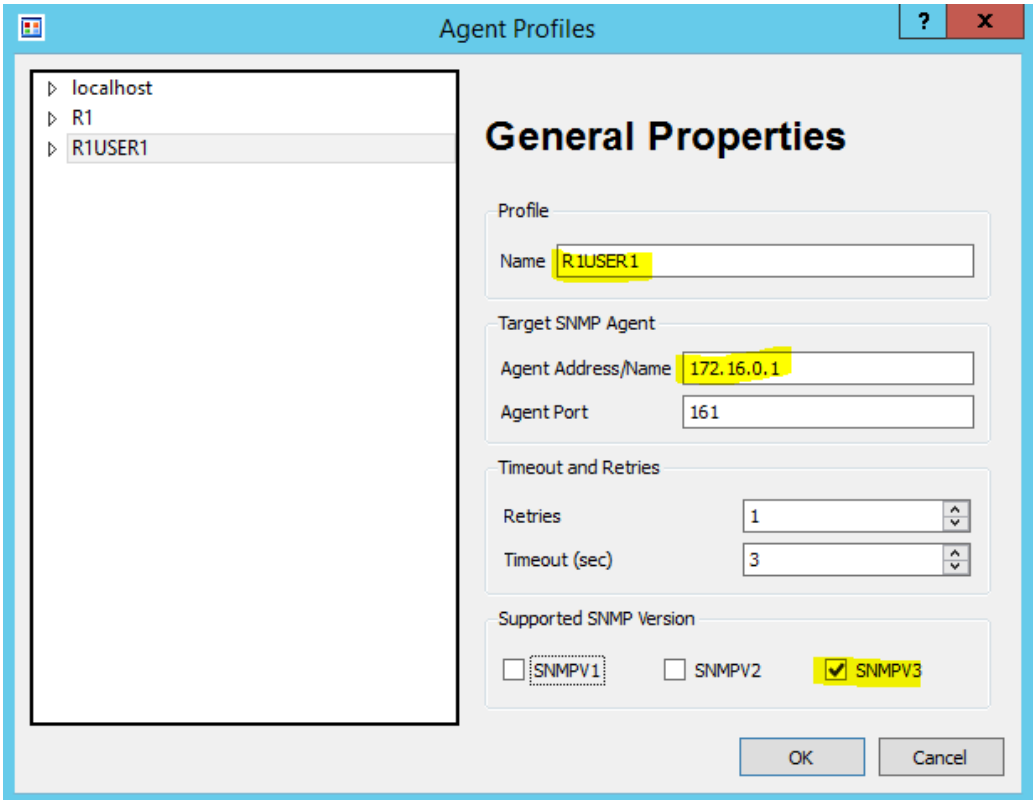


6. Create a profile with the following settings:

Name: **R1USER1**

Agent Address/Name: **172.16.0.1**

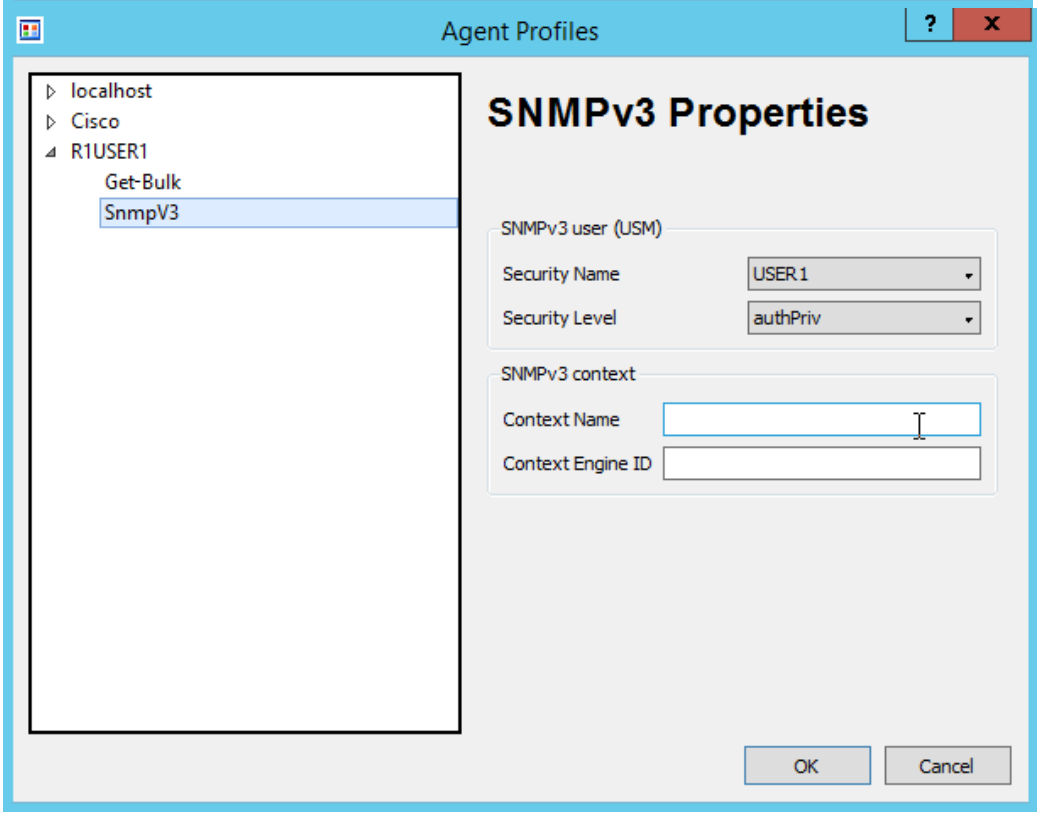
Supported SNMP Version: **SNMPv3**



Security Name: **USER1**

Security Level: **authPriv**

Note: Leave Context Name and Context Engine ID empty.

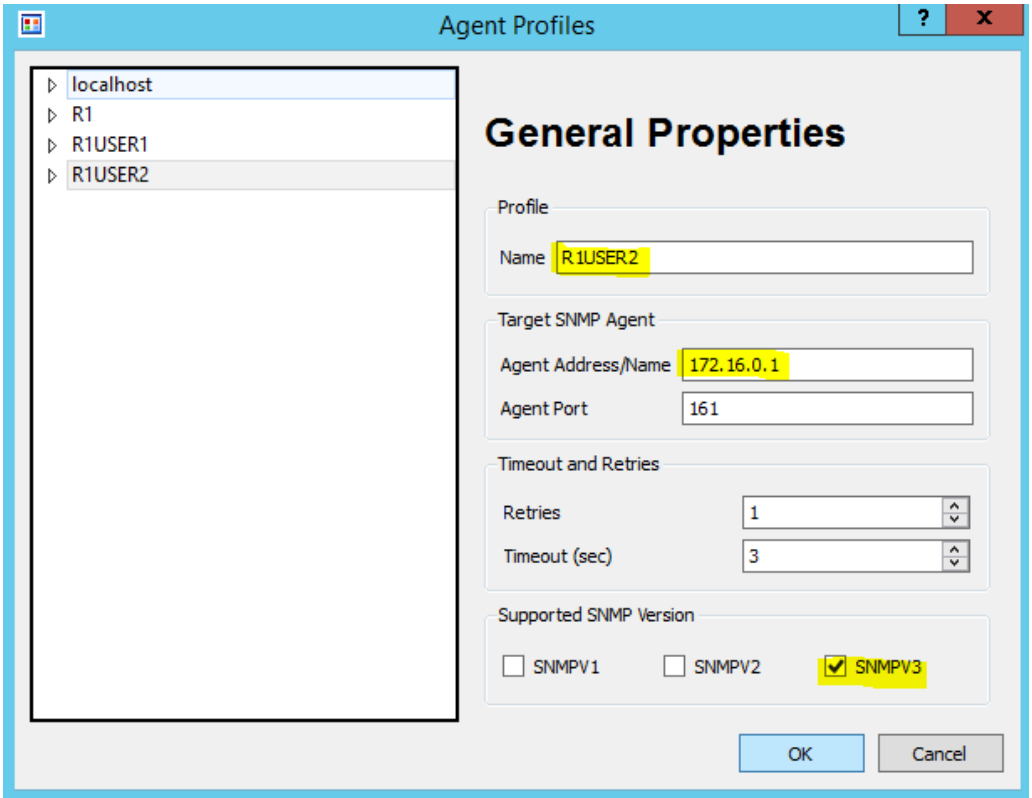


7. Create a profile with the following settings:

Name: **R1USER2**

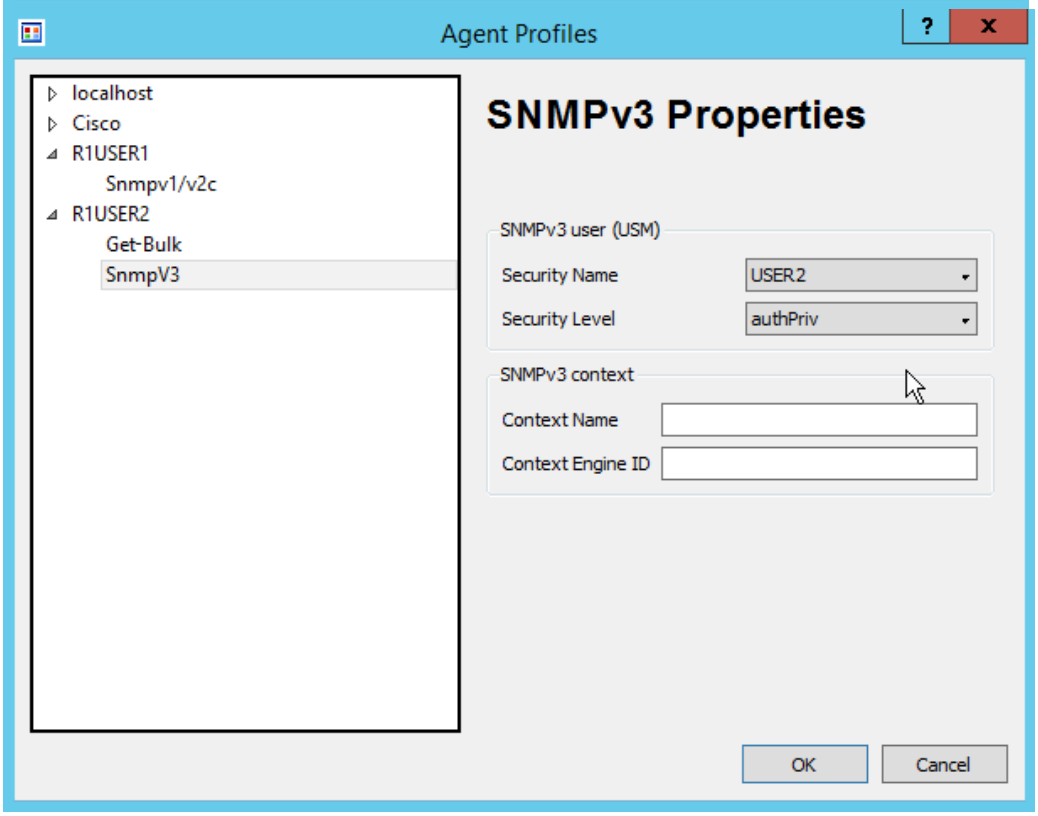
Agent Address/Name: **172.16.0.1**

Supported SNMP Version: **SNMPv3**

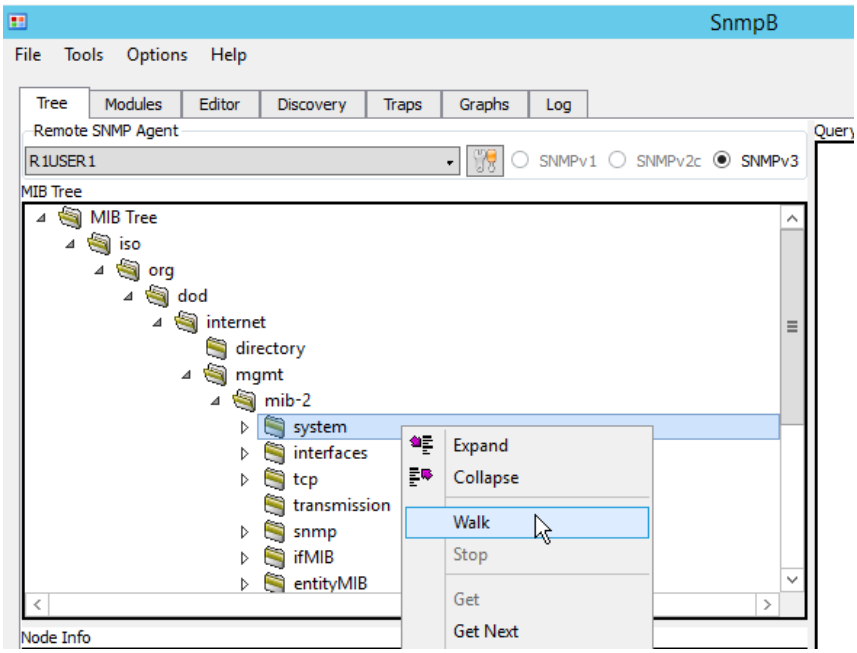


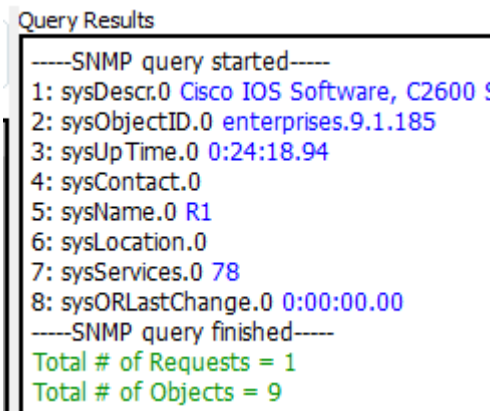
Security Name: **USER2**

Security Level: **authPriv**



8. Perform a Walk on **mib-2.system** using **R1USER1** agent profile.

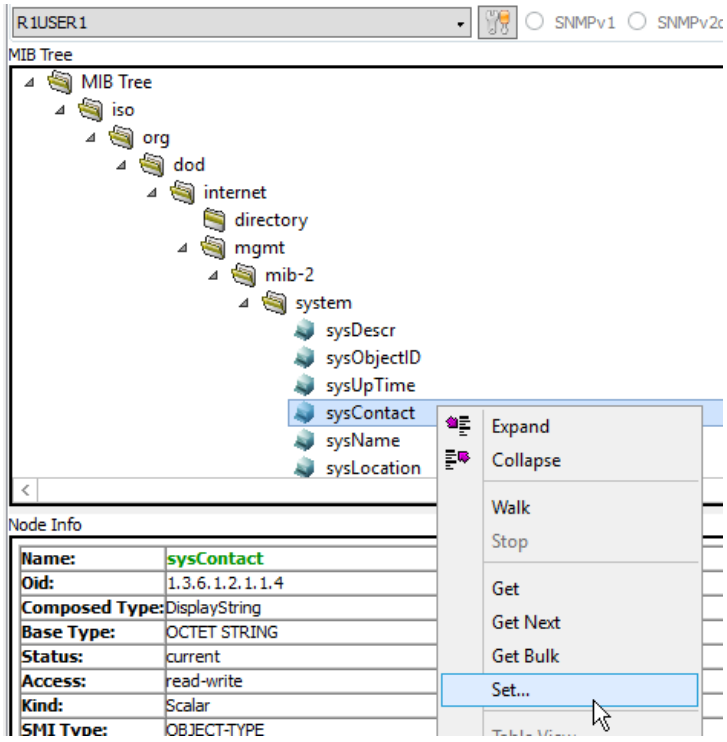


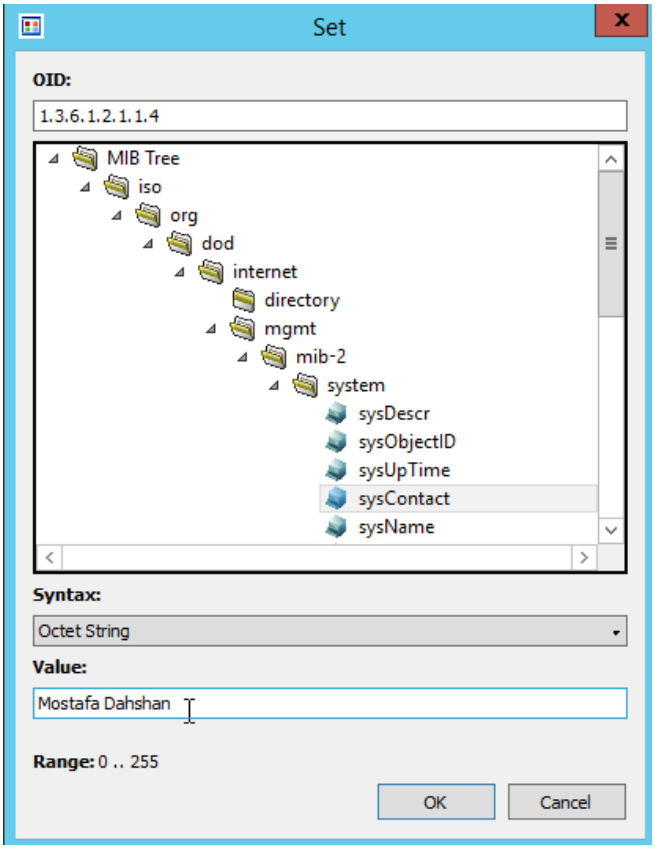


Note that the sysContact and sysLocation OIDs have empty values.

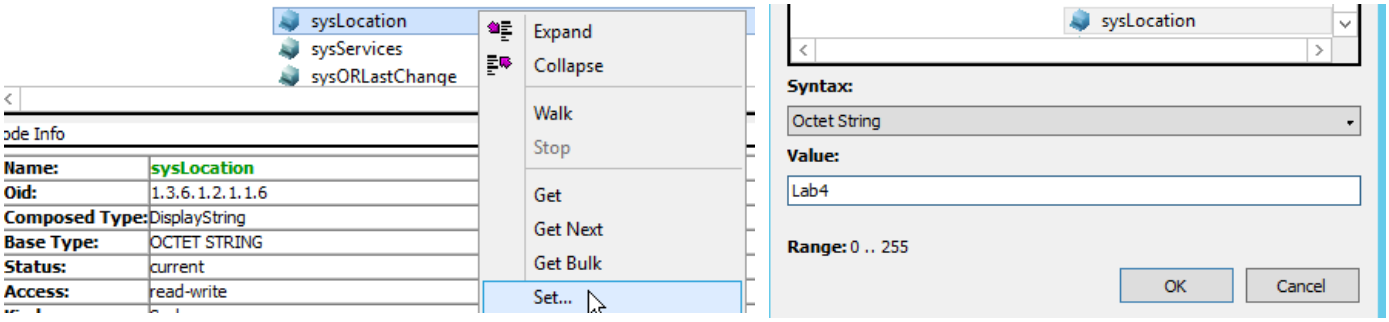
Lab sheet 3.2: provide a screenshot showing the output of system walk using R1USER1 agent profile.

9. Set the value of **sysContact** OID using **R1USER1** agent profile to **Your Name**.

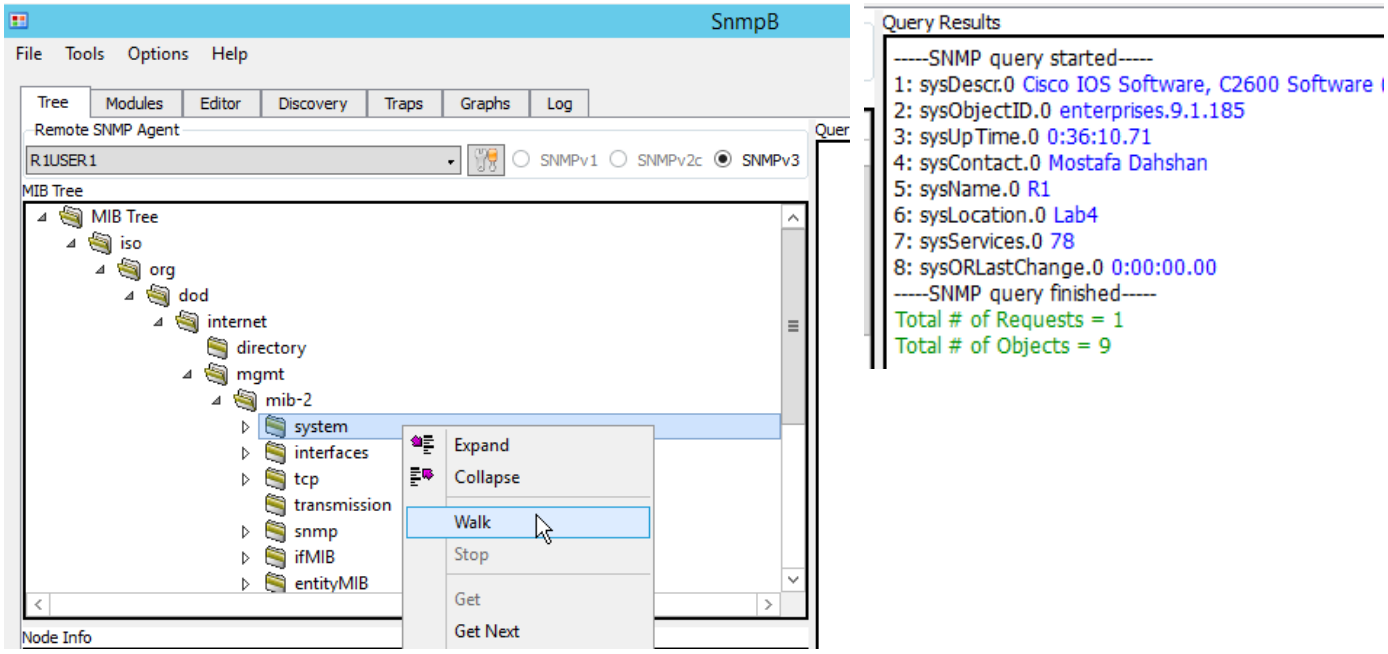




10. Set the value of **sysLocation** OID using **R1USER1** agent profile to **Lab4**.

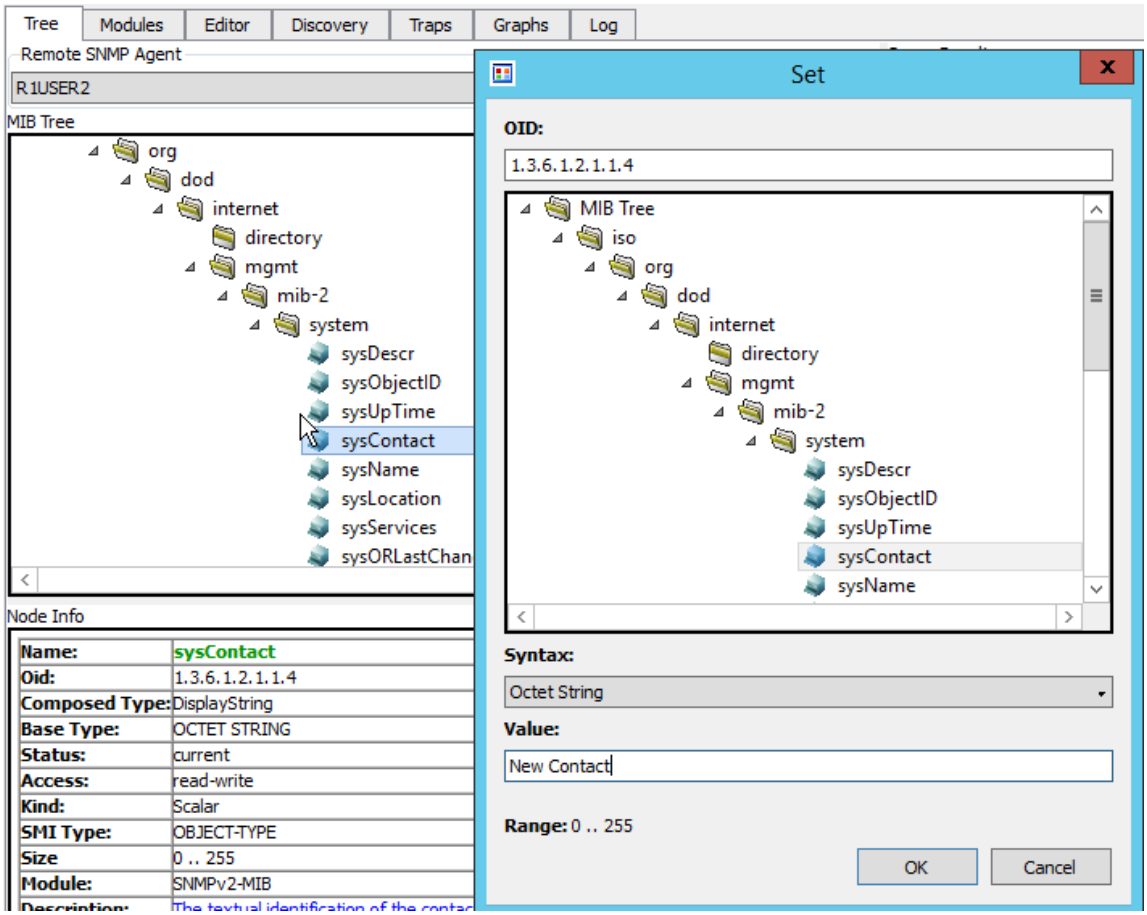


11. Perform a Walk on **mib-2.system** using **R1USER1** agent profile.

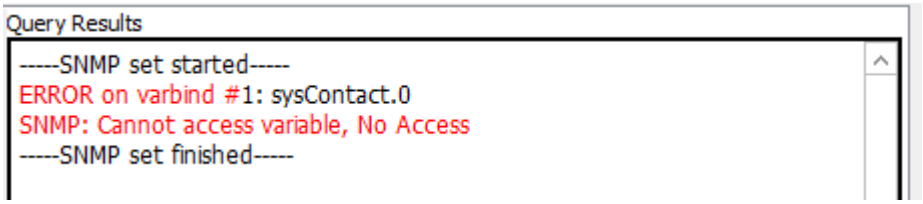


Lab sheet 3.3: provide a screenshot of the system walk after setting sysContact and sysLocation.

12. Attempt to set the value of **sysContact** OID. This time using **R1USER2** agent profile to **New Contact**.

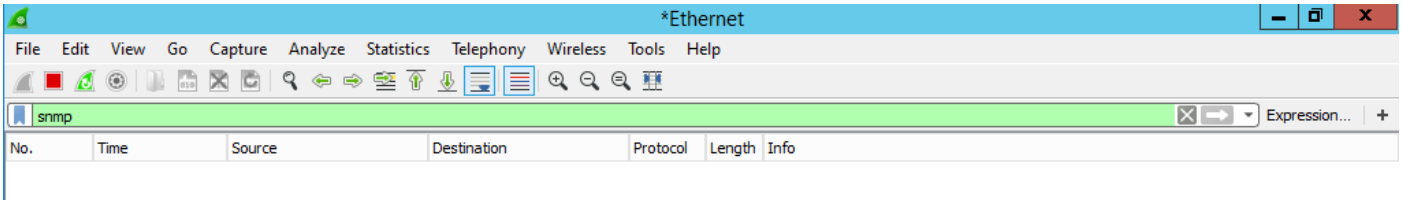


Note that the result indicates that it is not possible, because USER2 only has read access.

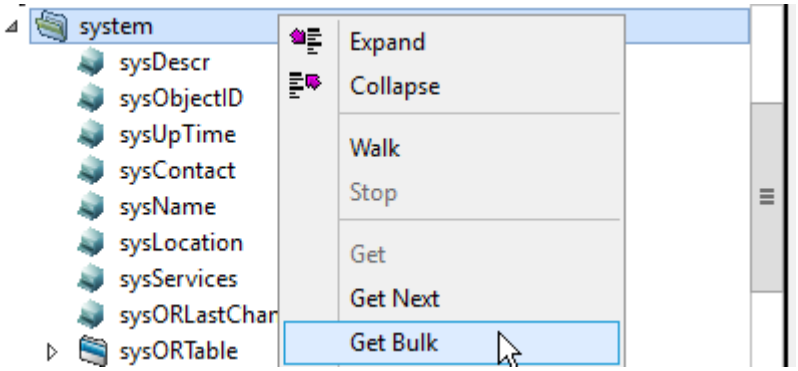


Part 4: Analyzing SNMPv3 traffic using Wireshark

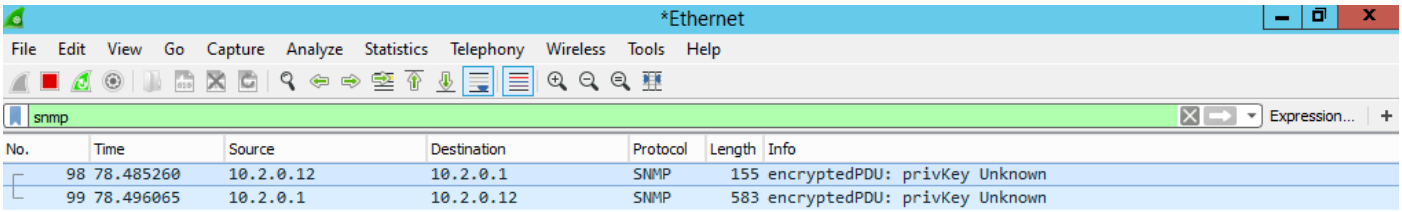
1. Run Wireshark as an Administrator and start capturing traffic on interface **Loop1** using filter **snmp**.



2. Using SnmpB, perform **GetBulk** on **mib-2.system** using **R1USER2** agent profile.

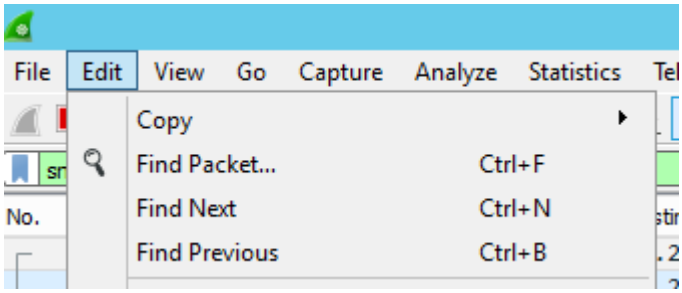


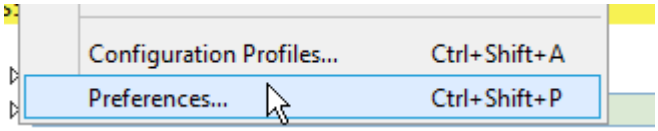
3. Check the Wireshark windows. Note that the PDU is encrypted and the privacy key is unknown to Wireshark.

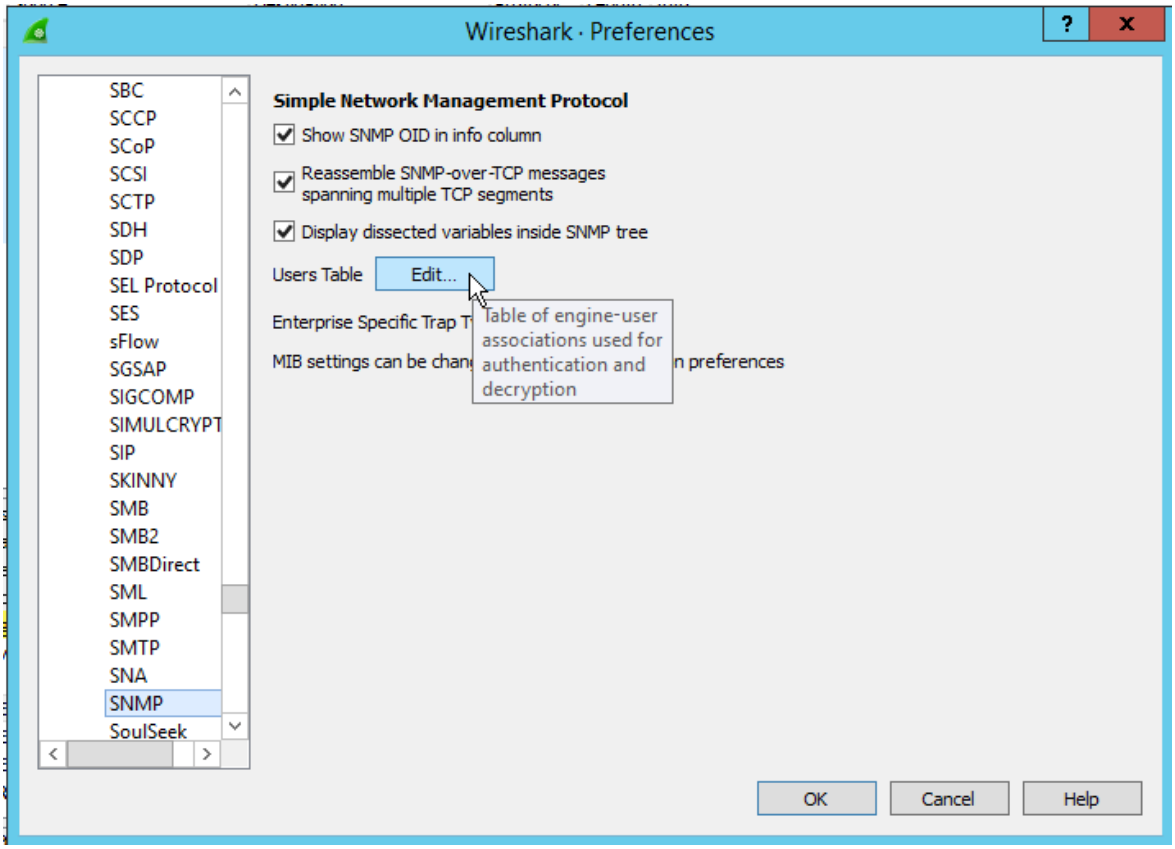


Lab sheet 4.1: provide a screenshot of Wireshark window showing privKey Unknown messages.

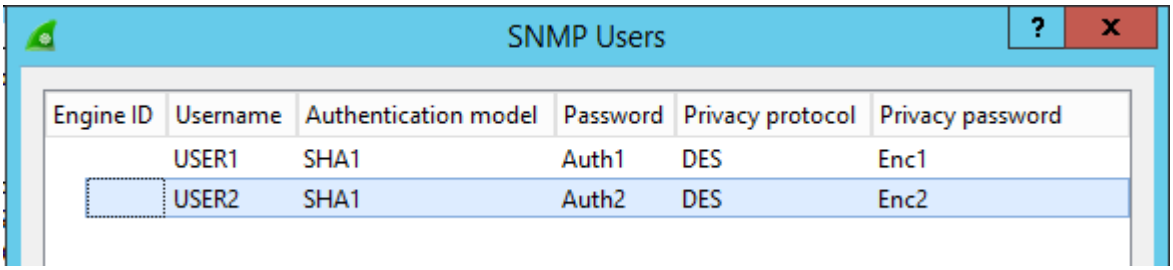
4. From Wireshark menu, click on **Edit-> Preferences**. Scroll down to **Protocols->SNMP** and click on **Edit** besides Users Table.



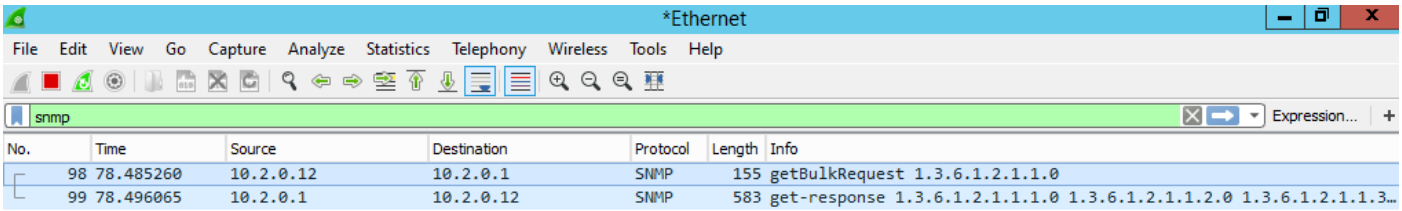




5. Add the information of USER1 and USER2.



6. Check the Wireshark window again. Note that Wireshark can now decrypt SNMP messages.



Lab sheet 4.2: provide a screenshot of Wireshark window showing the decrypted messages.