

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.

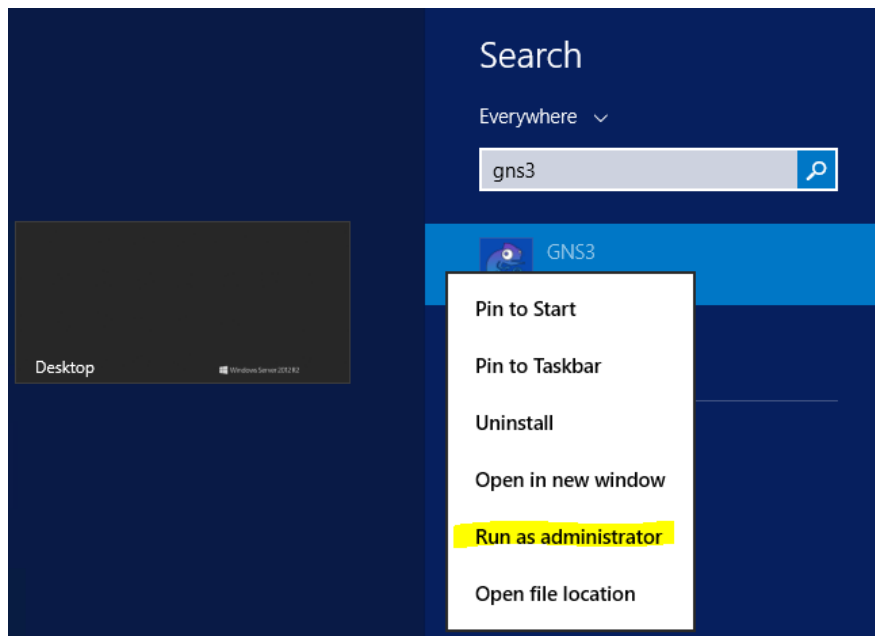
Part 1: Lab Setup

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.

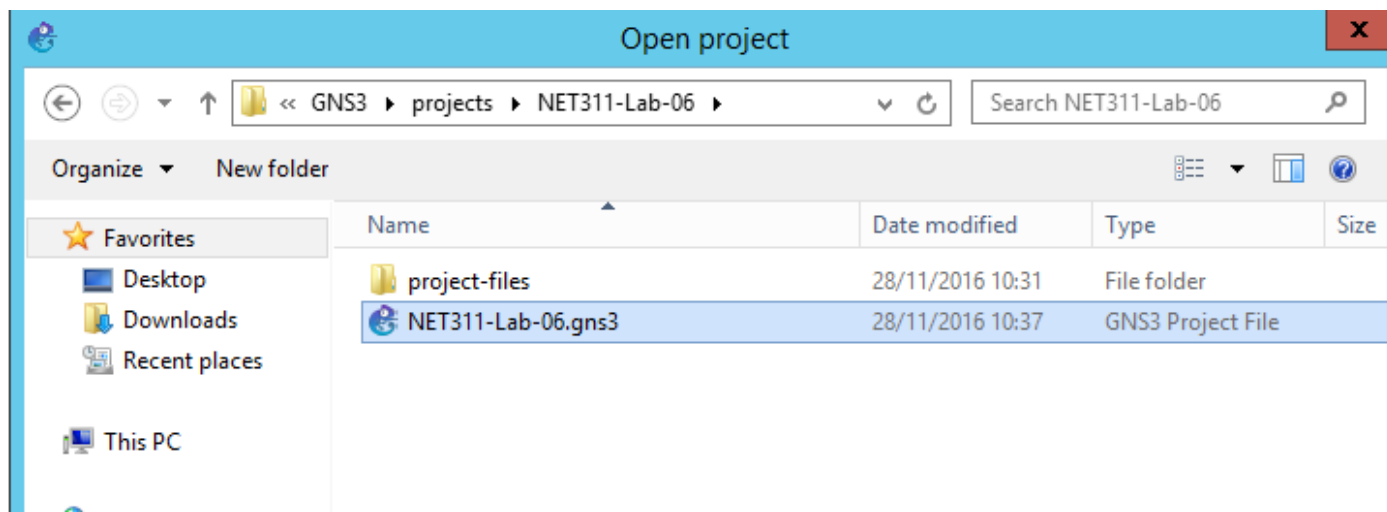
Part 2: SNMPv3 Security configuration on a Cisco router

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.

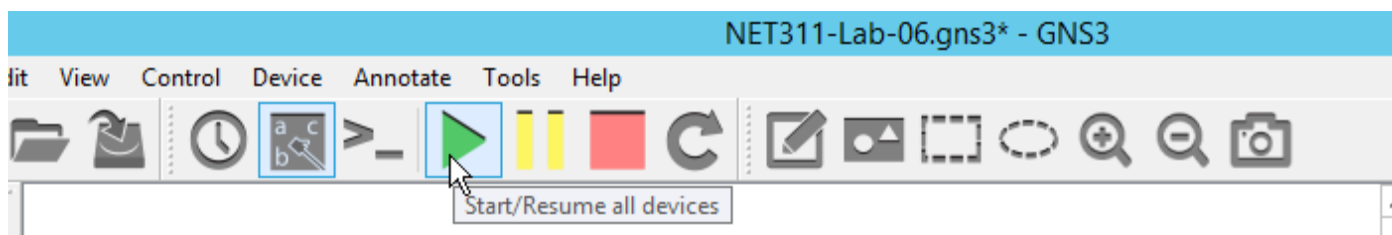
1. Run **GNS3** as an **administrator**.



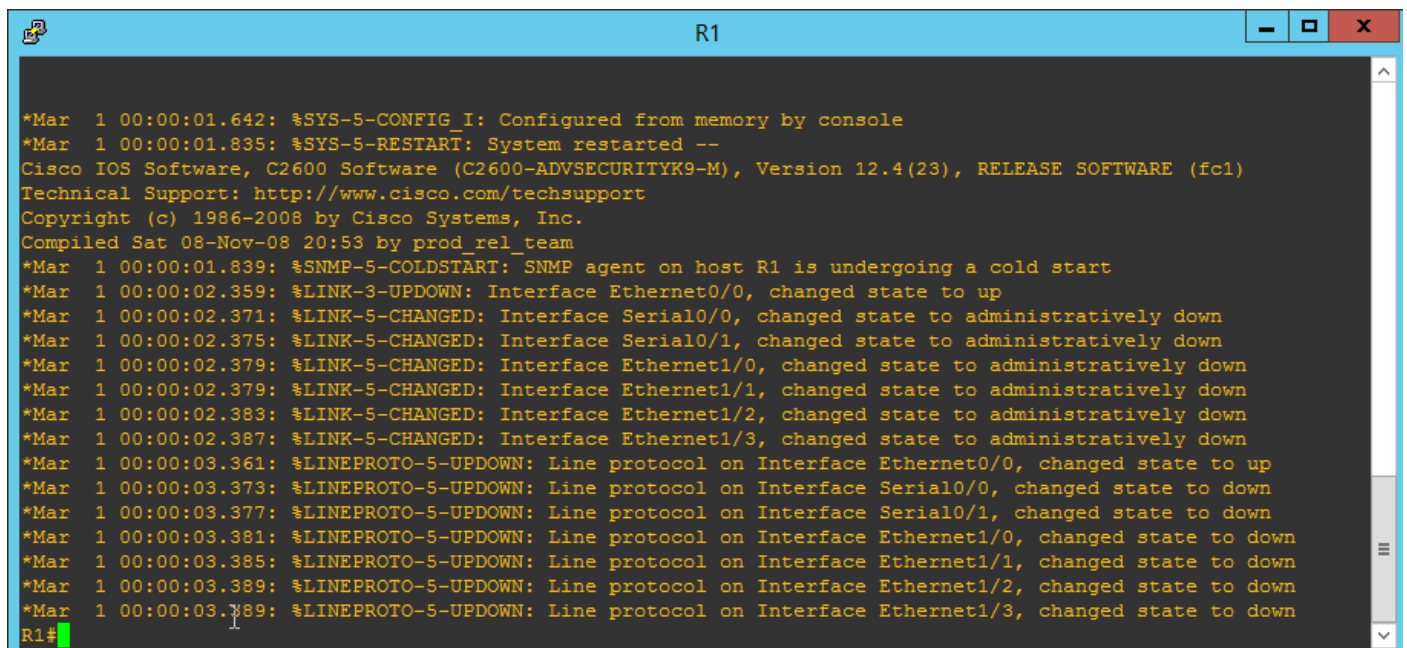
2. Open the GNS3 project **NET311-Lab-06.gns3**.



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.

A screenshot of a terminal window titled 'R1'. The window shows the output of a Cisco IOS system startup. The logs indicate a cold start of the SNMP agent and the state changes for various interfaces (Ethernet0/0, Serial0/0, Serial0/1, Ethernet1/0, Ethernet1/1, Ethernet1/2, Ethernet1/3) and line protocols. The prompt 'R1#' is visible at the bottom left of the terminal area.

```
*Mar 1 00:00:01.642: %SYS-5-CONFIG_I: Configured from memory by console
*Mar 1 00:00:01.835: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C2600 Software (C2600-ADVSECURITYK9-M), Version 12.4(23), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Sat 08-Nov-08 20:53 by prod_rel_team
*Mar 1 00:00:01.839: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a cold start
*Mar 1 00:00:02.359: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Mar 1 00:00:02.371: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down
*Mar 1 00:00:02.375: %LINK-5-CHANGED: Interface Serial0/1, changed state to administratively down
*Mar 1 00:00:02.379: %LINK-5-CHANGED: Interface Ethernet1/0, changed state to administratively down
*Mar 1 00:00:02.379: %LINK-5-CHANGED: Interface Ethernet1/1, changed state to administratively down
*Mar 1 00:00:02.383: %LINK-5-CHANGED: Interface Ethernet1/2, changed state to administratively down
*Mar 1 00:00:02.387: %LINK-5-CHANGED: Interface Ethernet1/3, changed state to administratively down
*Mar 1 00:00:03.361: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
*Mar 1 00:00:03.373: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
*Mar 1 00:00:03.377: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to down
*Mar 1 00:00:03.381: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
*Mar 1 00:00:03.385: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to down
*Mar 1 00:00:03.389: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2, changed state to down
*Mar 1 00:00:03.389: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/3, changed state to down
R1#
```

4. Configure the SNMPv3 engine ID.

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

5. Configure SNMPv3 views and groups.

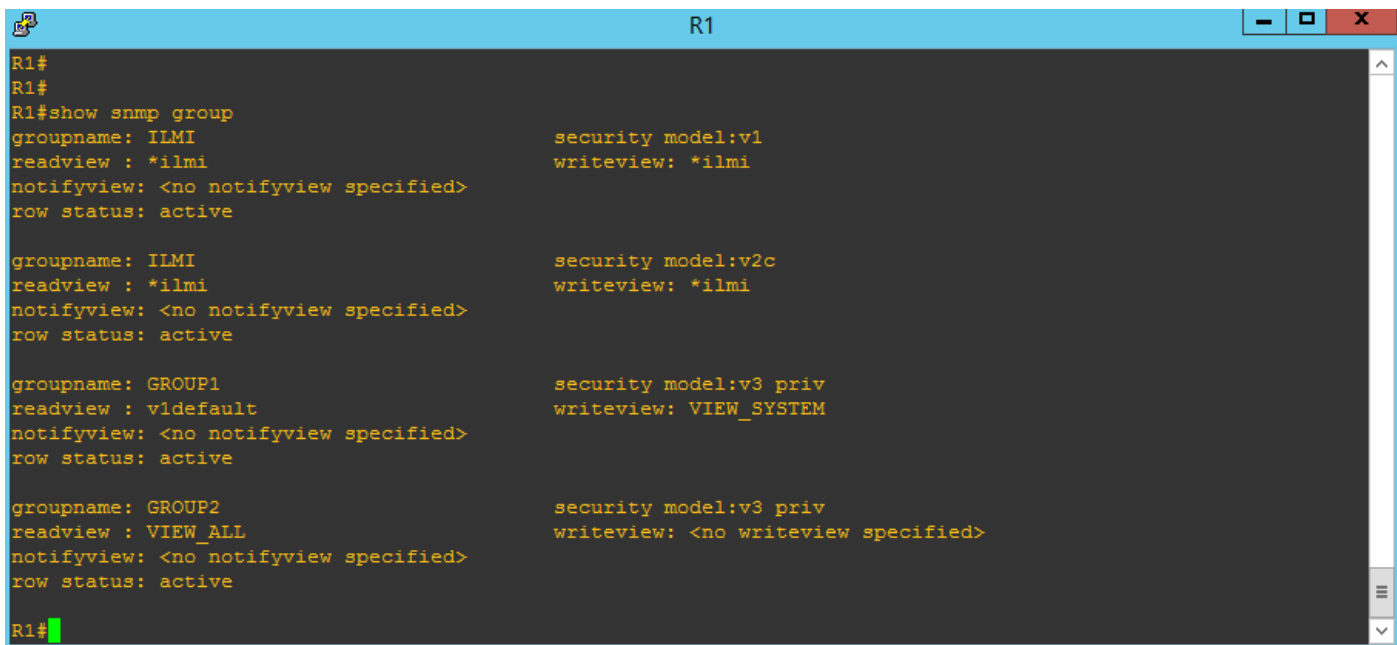
```
snmp-server engineID local 123456789A
snmp-server view VIEW_SYSTEM system included
snmp-server view VIEW_ALL iso included
snmp-server group GROUP1 v3 priv write VIEW_SYSTEM
snmp-server group GROUP2 v3 priv read VIEW_ALL
```

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
```



```
R1#
R1#
R1#show snmp group
groupname: ILMI                security model:v1
readview : *ilmi              writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                security model:v2c
readview : *ilmi              writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

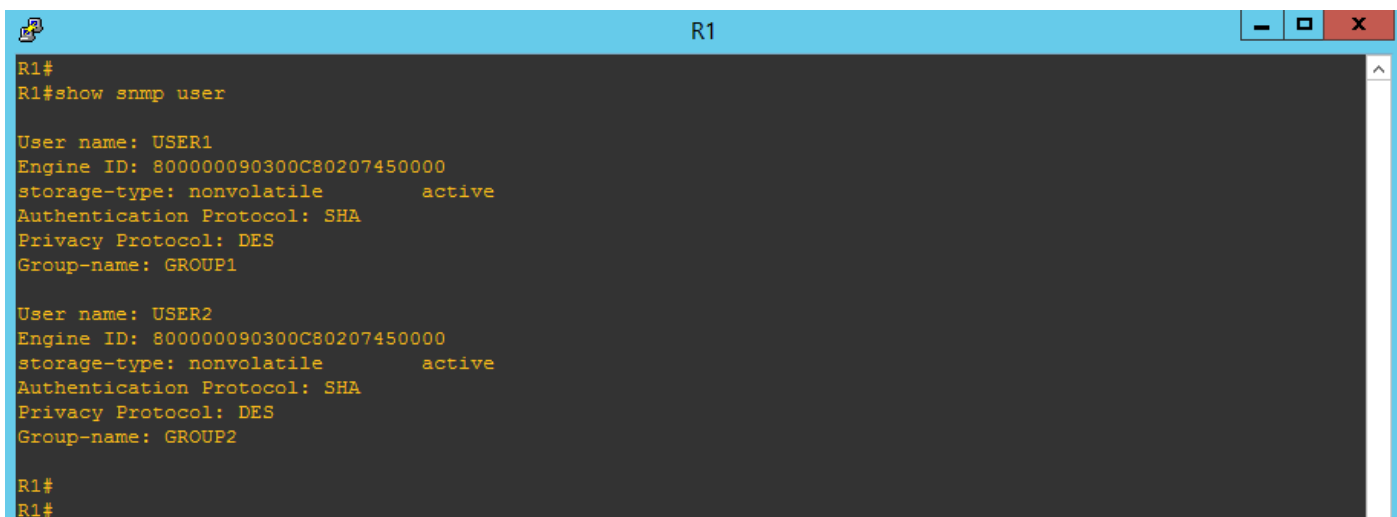
groupname: GROUP1              security model:v3 priv
readview : vldefault          writeview: VIEW_SYSTEM
notifyview: <no notifyview specified>
row status: active

groupname: GROUP2              security model:v3 priv
readview : VIEW_ALL           writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active
R1#
```

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
```



```
R1#
R1#show snmp user

User name: USER1
Engine ID: 800000090300C80207450000
storage-type: nonvolatile      active
Authentication Protocol: SHA
Privacy Protocol: DES
Group-name: GROUP1

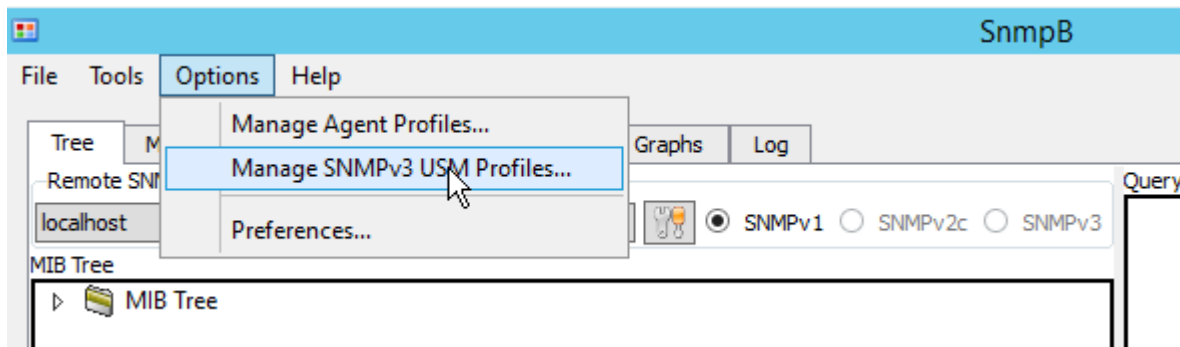
User name: USER2
Engine ID: 800000090300C80207450000
storage-type: nonvolatile      active
Authentication Protocol: SHA
Privacy Protocol: DES
Group-name: GROUP2

R1#
R1#
```

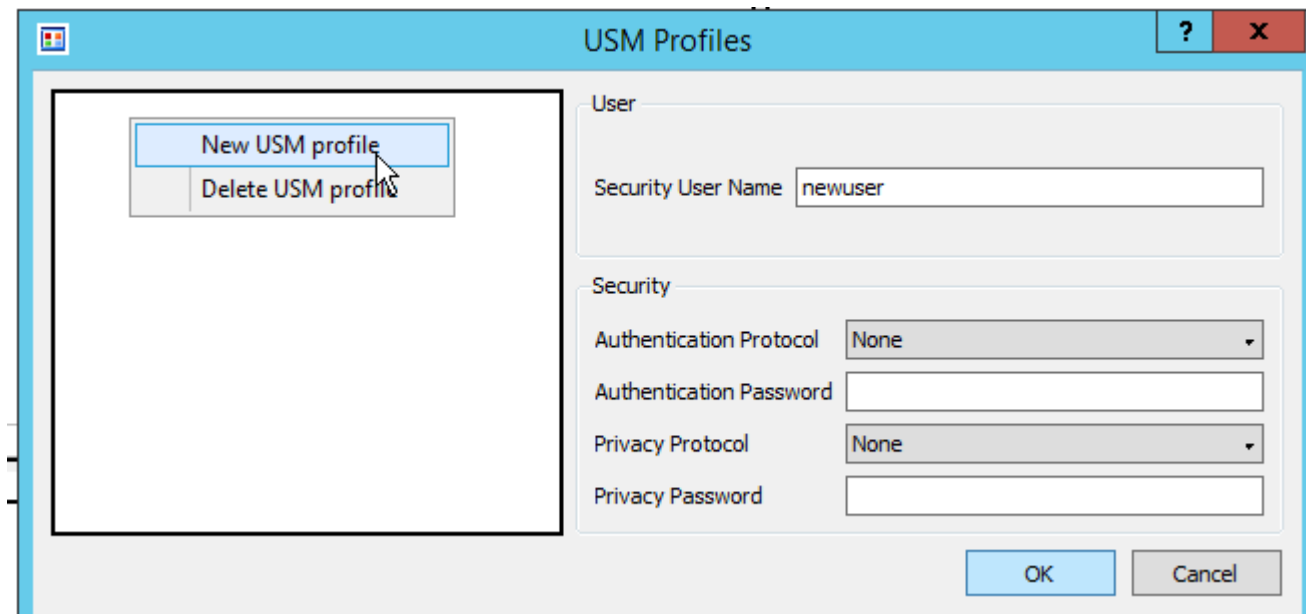
Lab sheet 2.2: provide a screenshot of the result of the show snmp user command.

Part 3: SNMPv3 USM Configuration on the SNMP manager

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



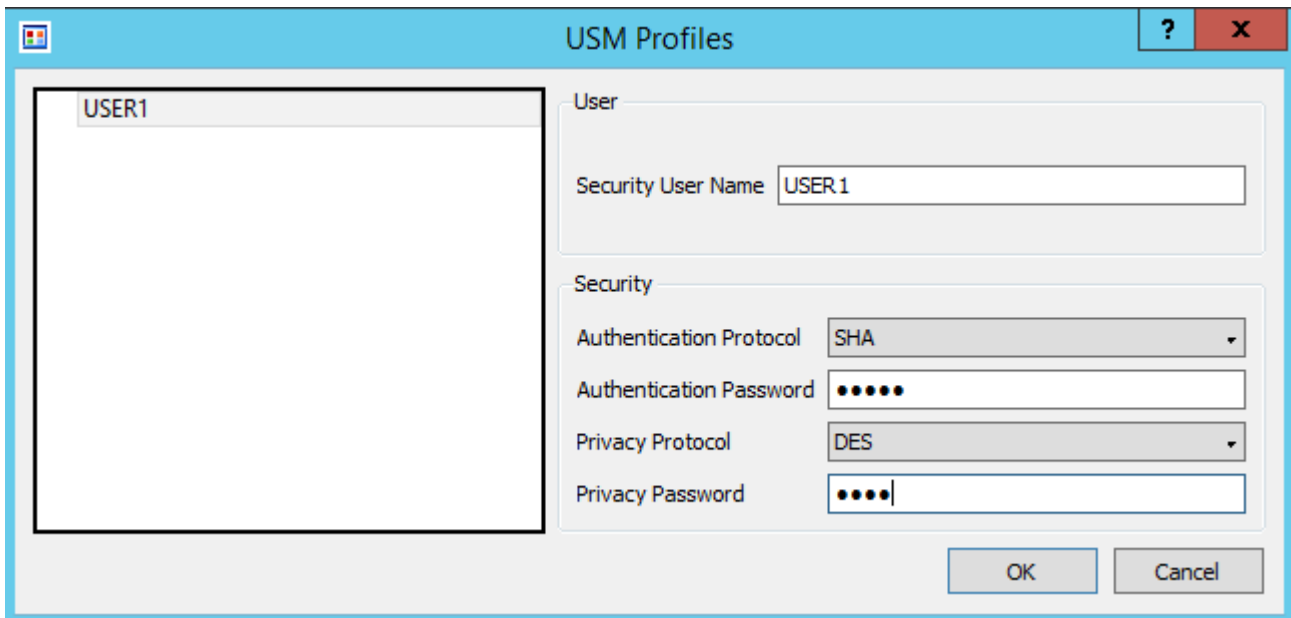
2. Right click and select New USM profile



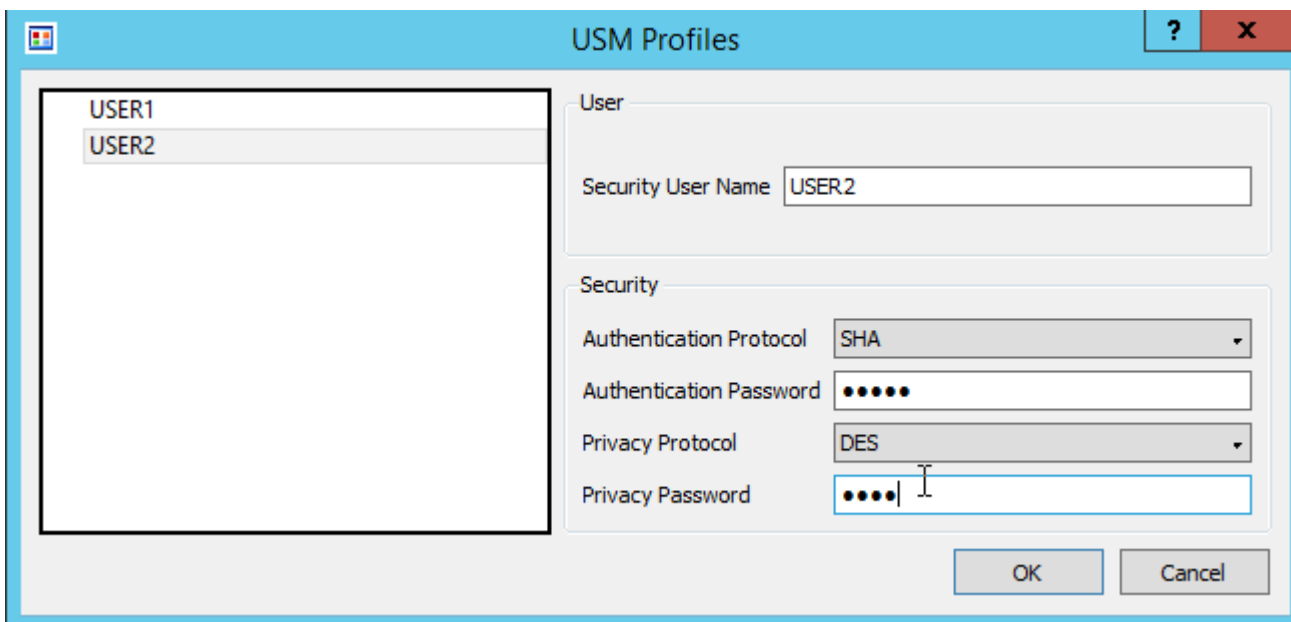
3. Create a profile for user **USER1** with the following settings:

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

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

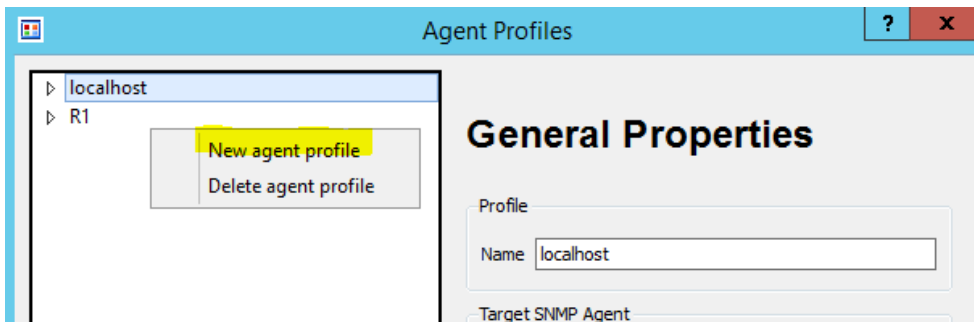


4. Create a profile for user **USER2** with the following settings:
 Select **SHA** for Authentication Protocol and **DES** for Privacy Protocol.
 Authentication password is **Auth2** and Privacy password is **Enc2**.



Lab sheet 3.1: provide a screenshot showing USM Profiles.

5. Create a new agent profile.

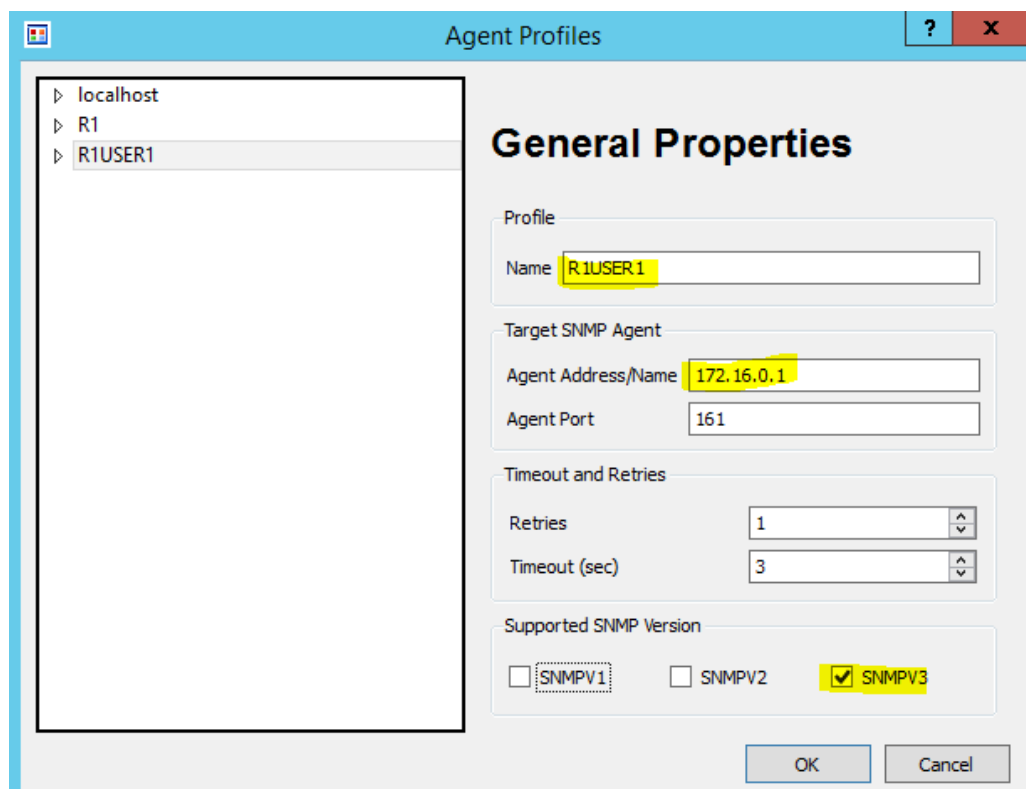


6. Create a profile with the following settings:

Name: **R1USER1**

Agent Address/Name:
172.16.0.1

Supported SNMP
Version: **SNMPv3**

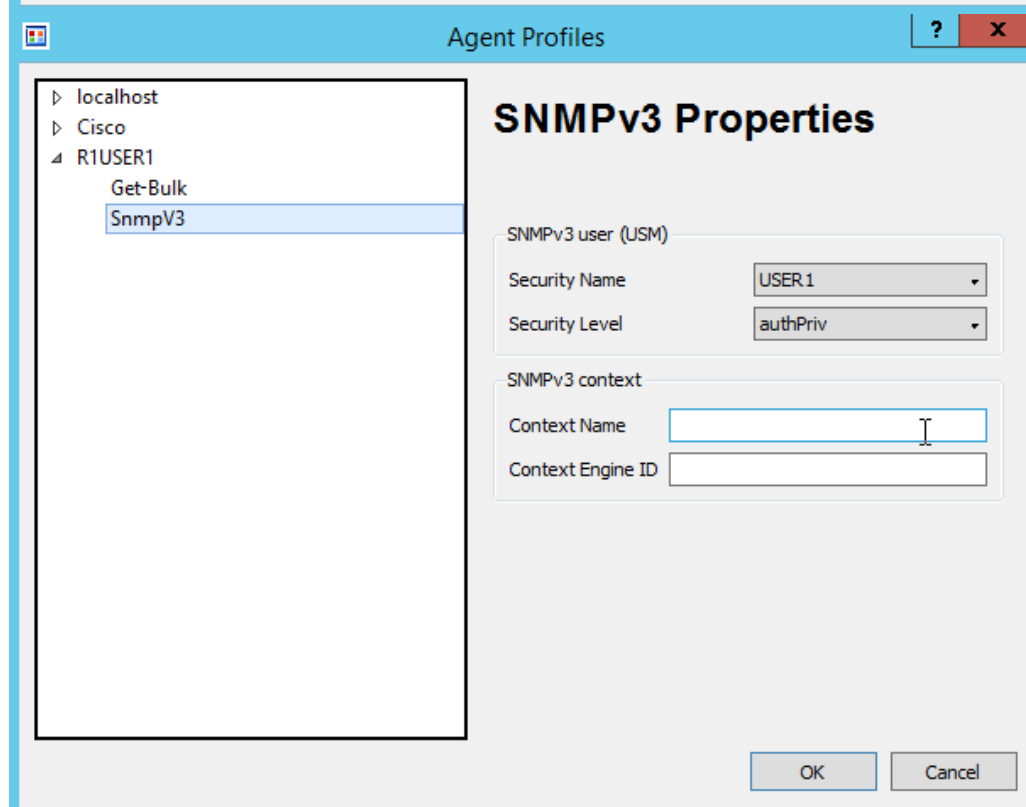


The 'Agent Profiles' dialog box shows the 'General Properties' tab. On the left, a tree view lists 'localhost', 'R1', and 'R1USER1'. The right pane contains the following fields: 'Profile Name' (R1USER1), 'Target SNMP Agent' section with 'Agent Address/Name' (172.16.0.1) and 'Agent Port' (161), 'Timeout and Retries' section with 'Retries' (1) and 'Timeout (sec)' (3), and 'Supported SNMP Version' section with checkboxes for 'SNMPV1', 'SNMPV2', and 'SNMPV3' (checked). 'OK' and 'Cancel' buttons are at the bottom right.

Security Name: **USER1**

Security Level: **authPriv**

Note: Leave Context
Name and Context
Engine ID empty.



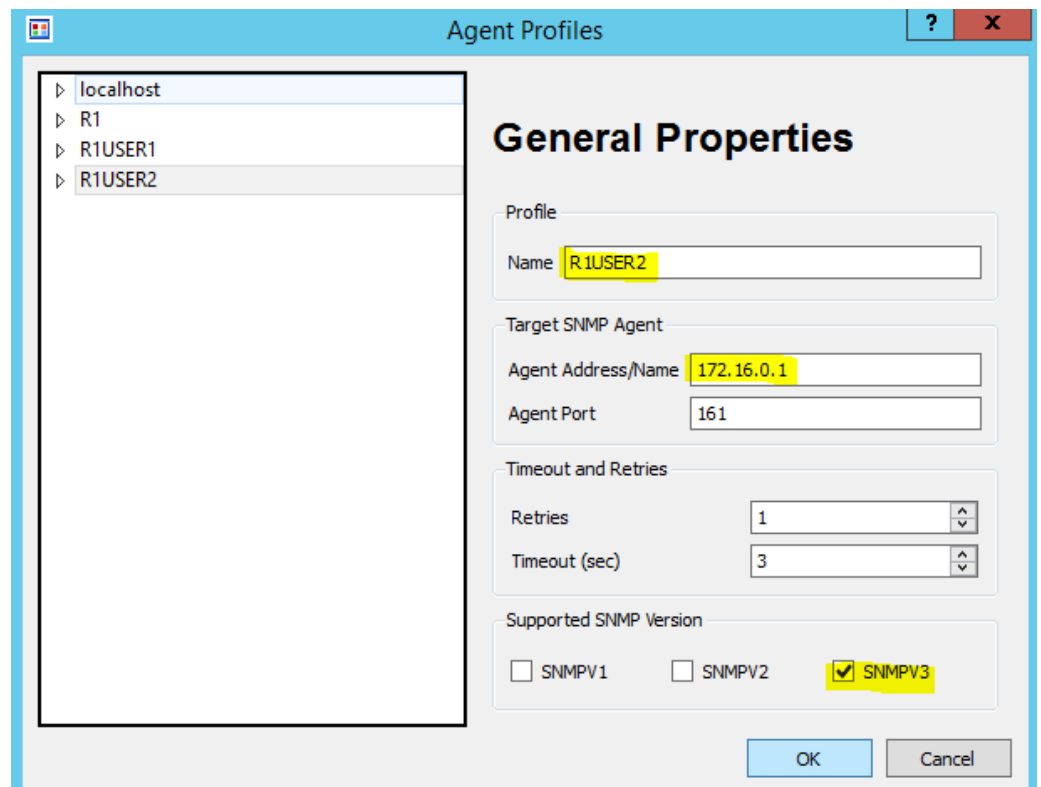
The 'Agent Profiles' dialog box shows the 'SNMPv3 Properties' tab. The left tree view is expanded to show 'R1USER1' with sub-items 'Get-Bulk' and 'SnmpV3'. The right pane contains: 'SNMPv3 user (USM)' section with 'Security Name' (USER1) and 'Security Level' (authPriv) dropdowns; and 'SNMPv3 context' section with 'Context Name' and 'Context Engine ID' text boxes. 'OK' and 'Cancel' buttons are at the bottom right.

7. Create a profile with the following settings:

Name: **R1USER2**

Agent Address/Name:
172.16.0.1

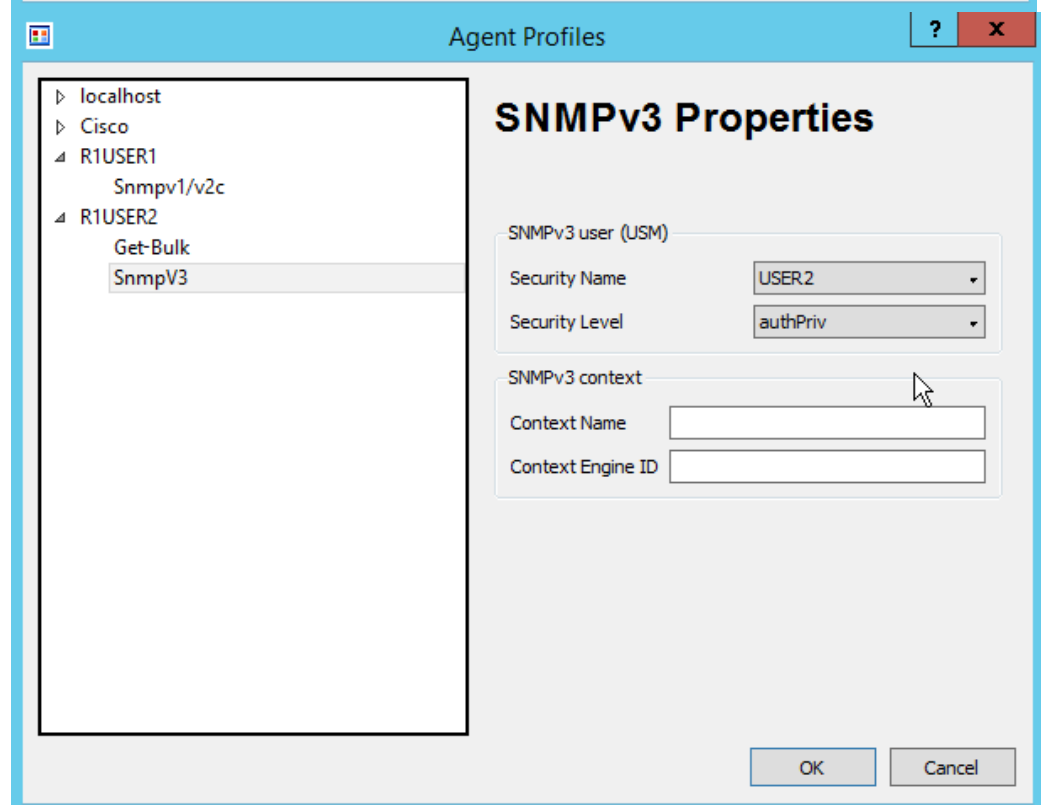
Supported SNMP
Version: **SNMPv3**



The 'Agent Profiles' dialog box shows the 'General Properties' tab. On the left, a tree view lists 'localhost', 'R1', 'R1USER1', and 'R1USER2', with 'R1USER2' selected. The right pane contains the following fields: 'Profile Name' (R1USER2), 'Target SNMP Agent' section with 'Agent Address/Name' (172.16.0.1) and 'Agent Port' (161), 'Timeout and Retries' section with 'Retries' (1) and 'Timeout (sec)' (3), and 'Supported SNMP Version' section with checkboxes for 'SNMPV1', 'SNMPV2', and 'SNMPV3' (checked). 'OK' and 'Cancel' buttons are at the bottom right.

Security Name: **USER2**

Security Level: **authPriv**



The 'Agent Profiles' dialog box shows the 'SNMPv3 Properties' tab. The left tree view is expanded to show 'R1USER2' with sub-items 'Get-Bulk' and 'SnmpV3', which is selected. The right pane contains: 'SNMPv3 user (USM)' section with 'Security Name' (USER2) and 'Security Level' (authPriv) dropdowns; and 'SNMPv3 context' section with 'Context Name' and 'Context Engine ID' text boxes. 'OK' and 'Cancel' buttons are at the bottom right.

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

The screenshot shows the SnmpB application interface. The 'Tree' tab is active, displaying the MIB Tree structure. The 'Remote SNMP Agent' is set to 'R1USER1'. The 'MIB Tree' shows the hierarchy: iso -> org -> dod -> internet -> directory -> mgmt -> mib-2 -> system. A right-click context menu is open over the 'system' node, with the 'Walk' option selected. To the right, the 'Query Results' window displays the output of the walk operation:

```
-----SNMP query started-----
1: sysDescr.0 Cisco IOS Software, C2600 !
2: sysObjectID.0 enterprises.9.1.185
3: sysUpTime.0 0:24:18.94
4: sysContact.0
5: sysName.0 R1
6: sysLocation.0
7: sysServices.0 78
8: sysORLastChange.0 0:00:00.00
-----SNMP query finished-----
Total # of Requests = 1
Total # of Objects = 9
```

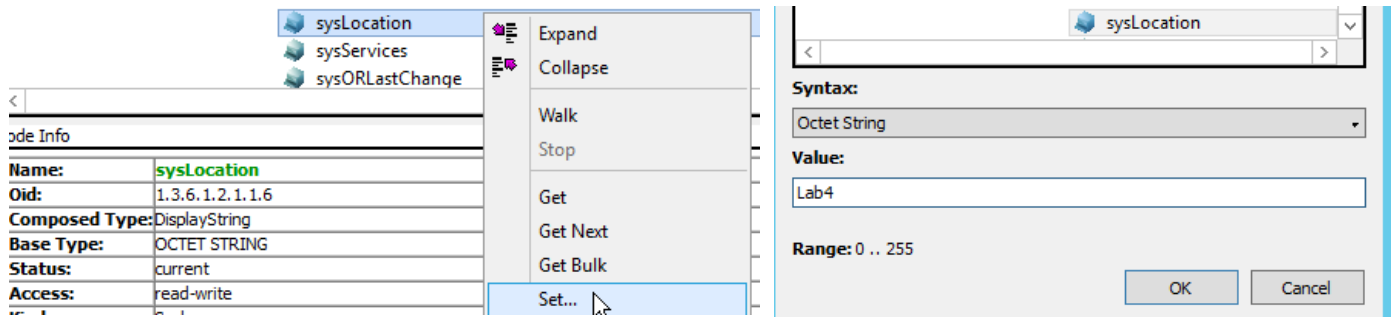
Note that the sysContact and sysLocation OIDs have empty values.

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

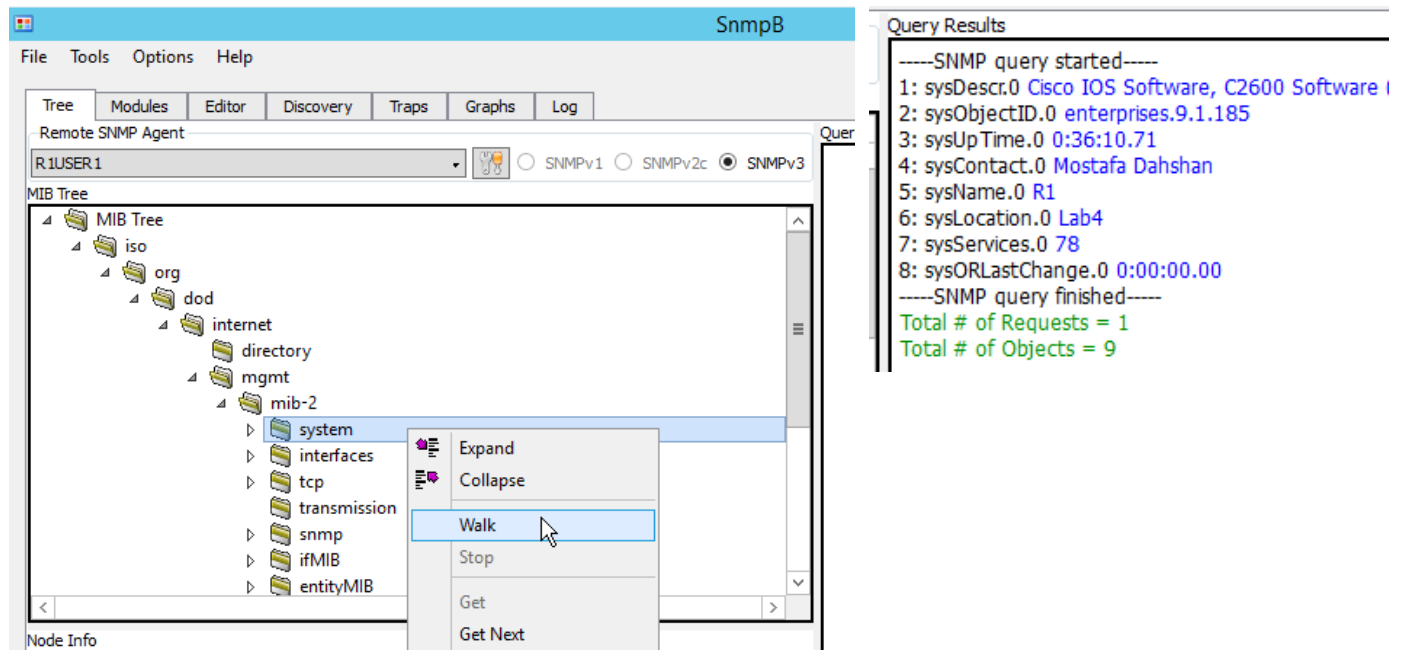
9. Set the value of **sysContact** OID using **R1USER1** agent profile to **Your Name**.

The screenshot shows the SnmpB application interface. The 'Tree' tab is active, displaying the MIB Tree structure. The 'Remote SNMP Agent' is set to 'R1USER1'. The 'MIB Tree' shows the hierarchy: iso -> org -> dod -> internet -> directory -> mgmt -> mib-2 -> system. The 'sysContact' node is selected. A right-click context menu is open over the 'sysContact' node, with the 'Set...' option selected. To the right, the 'Set' dialog box is open, showing the 'OID' field with the value '1.3.6.1.2.1.1.4'. The 'Syntax' field is set to 'Octet String'. The 'Value' field contains the text 'Mostafa Dahshan'. The 'Range' field shows '0 .. 255'. The 'OK' and 'Cancel' buttons are at the bottom right.

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**.

The screenshot shows the NetMiner interface with the 'Set' dialog box open. The 'Remote SNMP Agent' is set to 'R1USER2'. The 'MIB Tree' on the left shows the hierarchy: org > dod > internet > directory > mgmt > mib-2 > system. The 'sysContact' node is selected. The 'Node Info' panel shows the following details for 'sysContact':

Name:	sysContact
Oid:	1.3.6.1.2.1.1.4
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:	The textual identification of the contact

The 'Set' dialog box has the following fields:

- OID:** 1.3.6.1.2.1.1.4
- MIB Tree:** The same hierarchy as the left panel, with 'sysContact' selected.
- Syntax:** Octet String
- Value:** New Contact
- Range:** 0 .. 255
- Buttons:** OK, Cancel

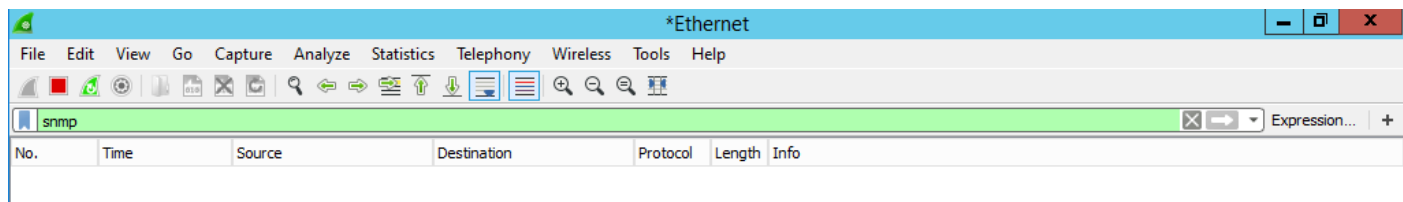
Note that the result indicates that it is not possible, because USER2 only has read access.

The 'Query Results' window displays the following text:

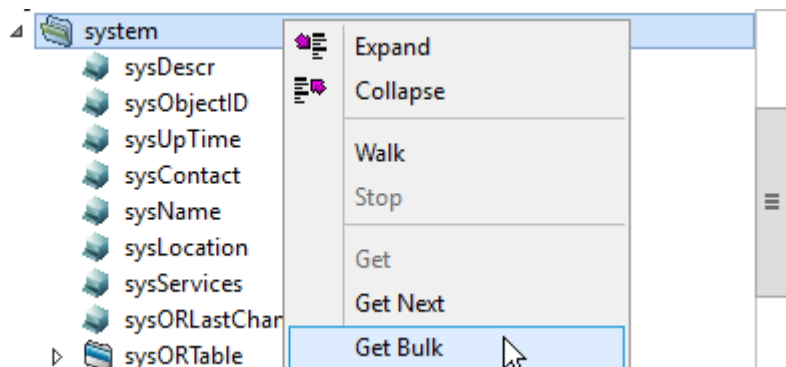
```
-----SNMP set started-----  
ERROR on varbind #1: sysContact.0  
SNMP: Cannot access variable, No Access  
-----SNMP set finished-----
```

Part 4: Analyzing SNMPv3 traffic using Wireshark

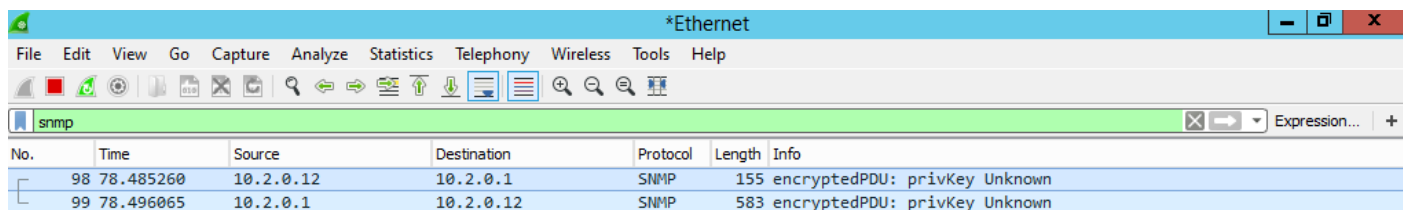
1. Run Wireshark as an Administrator and start capturing traffic on interface **Loop1** using filter **snmp**.



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

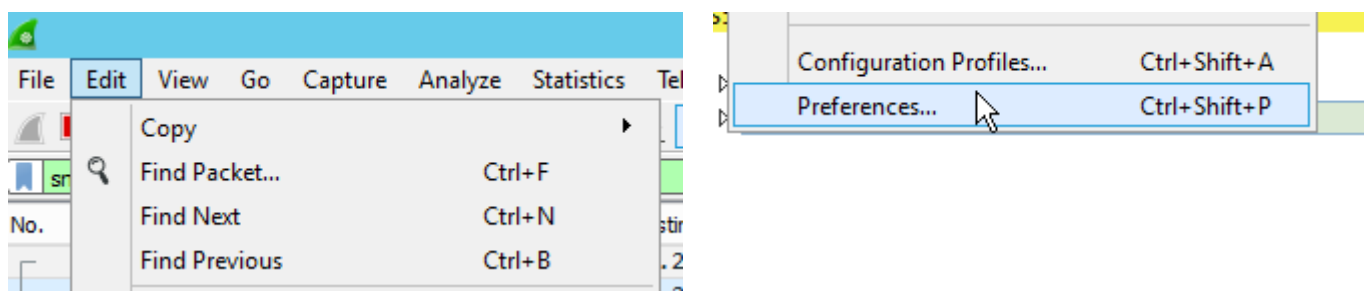


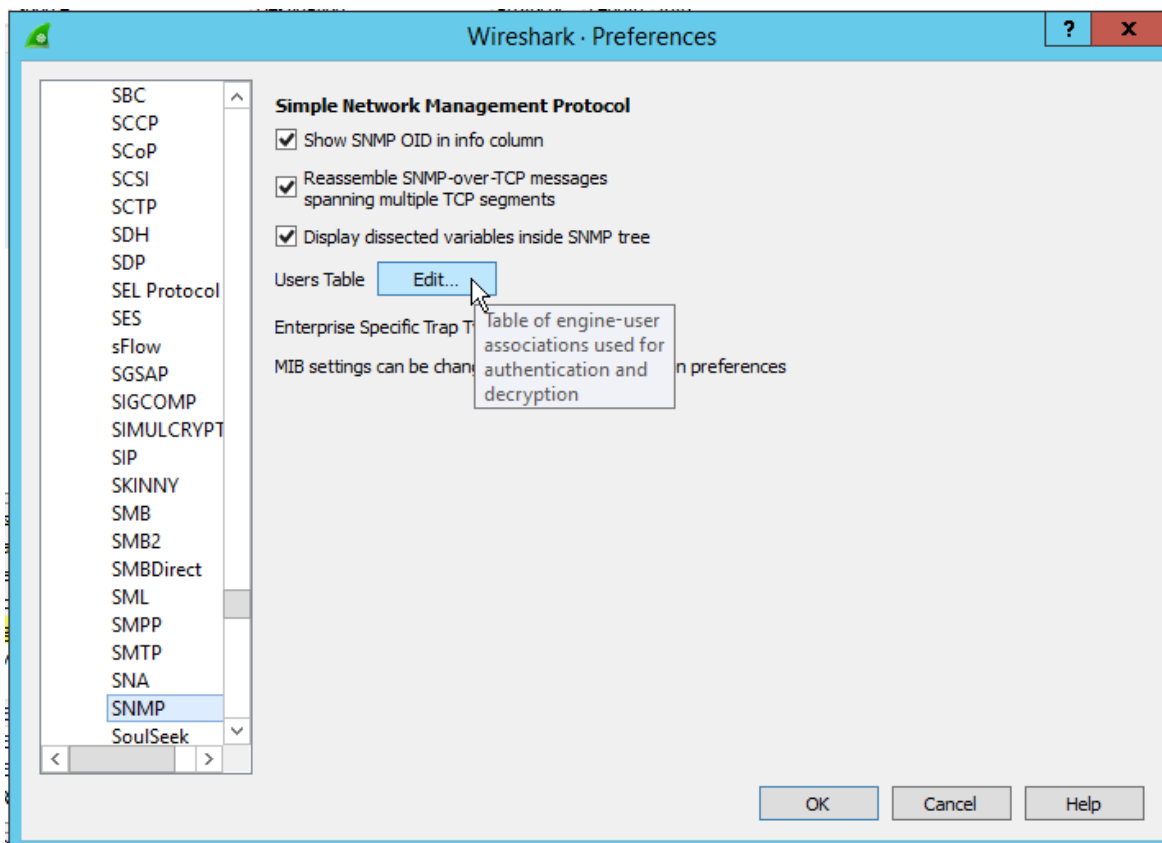
3. Check the Wireshark windows. Note that the PDU is encrypted and the privacy key is unknown to Wireshark.



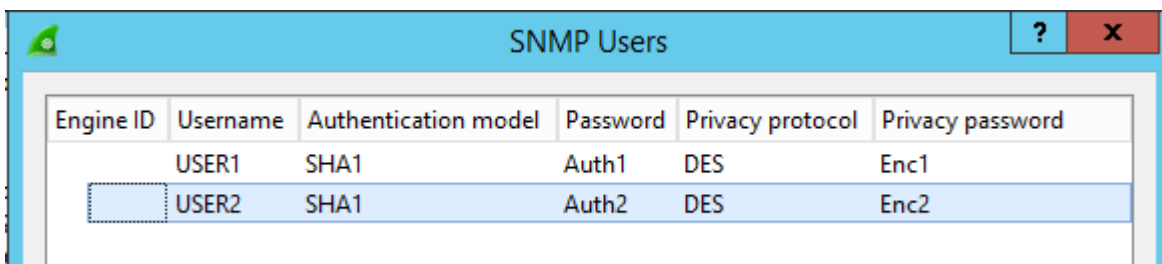
Lab sheet 4.1: provide a screenshot of Wireshark window showing privKey Unknown messages.

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

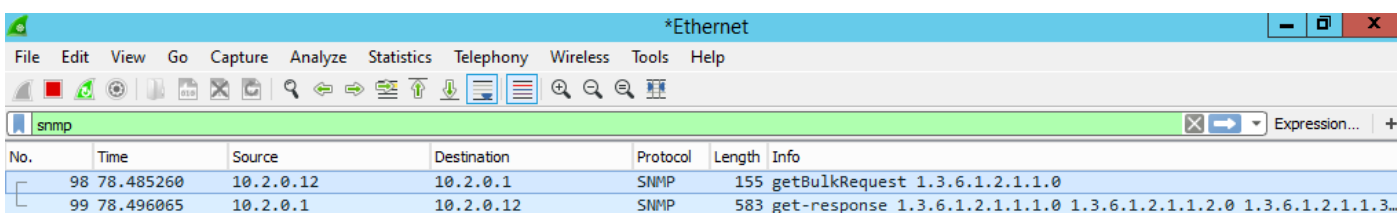




5. Add the information of USER1 and USER2.



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.