Lab 7: SNMP PDU Formats

NET311 - Computer Networks Management

Instructor: Dr. Mostafa Dahshan

## Objectives

1. Deeper understanding of SNMPv2 and SNMPv3 protocols.
2. Analyzing the formats of different SNMPv2 and SNMPv3 PDUs.

## References

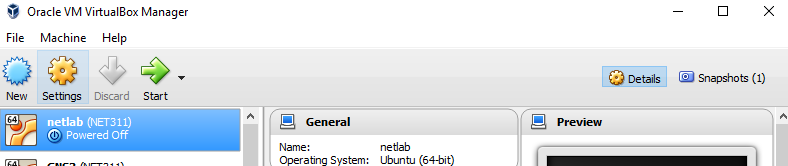
1. [Using CORE Network Emulator GUI](http://www.linuxintro.org/wiki/Netcat).
2. [CORE Network Emulator: Video Tutorials](http://www.nrl.navy.mil/itd/ncs/products/core/demo5).
3. [CORE Network Emulator: Install Network Services](http://www.brianlinkletter.com/core-network-emulator-install-network-services/).
4. [Manpage of snmpd.conf Examples](http://net-snmp.sourceforge.net/docs/man/snmpd.examples.html).
5. [VACM: Net-snmp tutorials](http://www.net-snmp.org/wiki/index.php/Vacm).
6. [VACM (Access Control) configuration](http://www.net-snmp.org/tutorial/tutorial-5/demon/vacm/).
7. [Manpage of snmpset](http://www.net-snmp.org/docs/man/snmpset.html).
8. [Manpage of snmpbulkget.](http://www.net-snmp.org/docs/man/snmpbulkget.html)
9. [netcat - Linuxintro](http://www.linuxintro.org/wiki/Netcat).

## Instructions

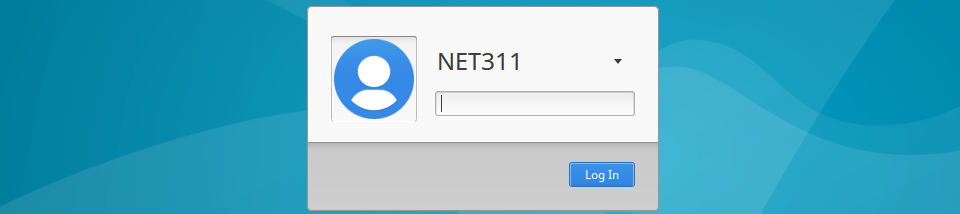
1. Read the lab instructions.
2. Provide question answers and screenshots in the supplied answer sheet.
3. After finishing the lab, upload your saved answer sheet to LMS.

# Part 1: Start the Network Environment

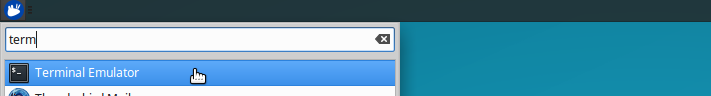
1. Start the netlab Linux virtual machine.



2. Login to the netlab Linux virtual machine using login: **net311** password: **abc.311**

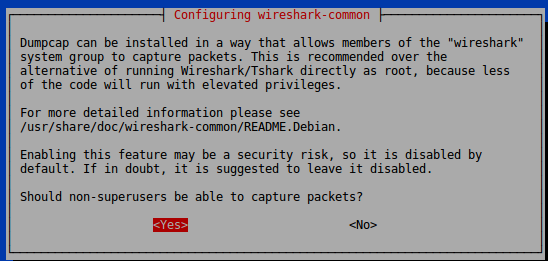


3. Run the **Terminal emulator**



4. To allow access to wireshark, run the following command

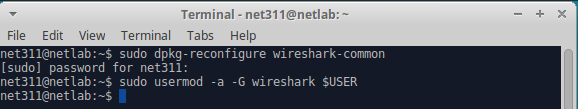
sudo dpkg-reconfigure wireshark-common



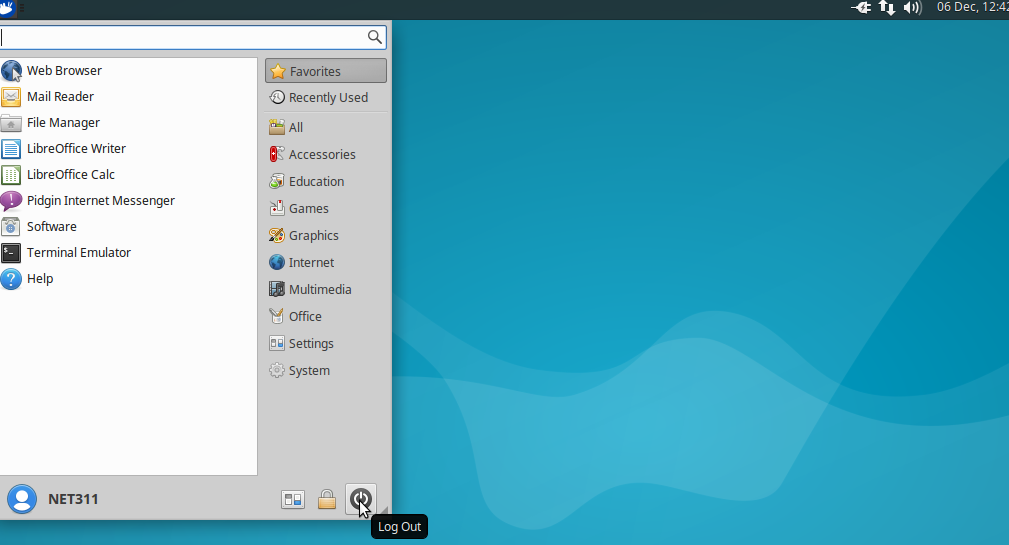
5. Click Yes.

6. Run the following command

sudo usermod -a -G wireshark $USER

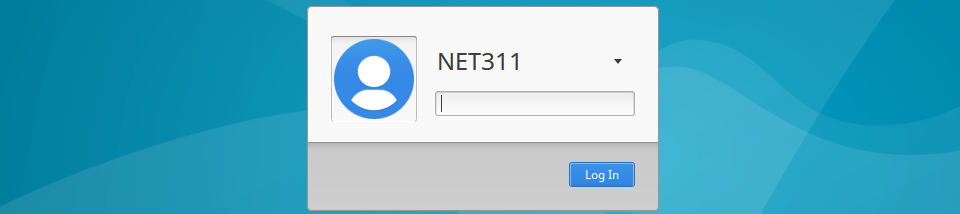


7. Log out.





8. Log in again with the password: **abc.311**



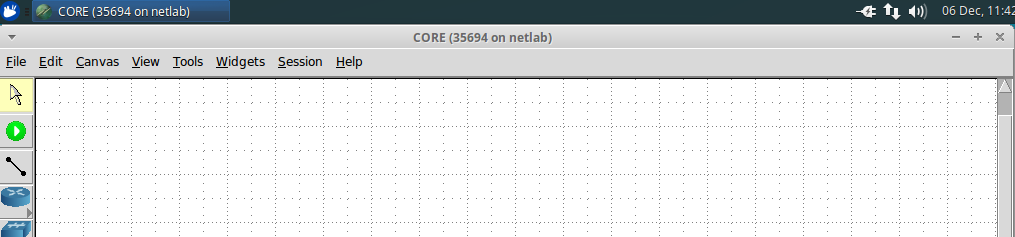
9. Locate the file **NET311-Lab-07.imn** included in the lab files. Copy the file to the desktop of the virtual machine.

If you can't use drag-and-drop, you may copy the file contents into a text file using **Mousepad**. Save the new file under the Desktop folder with the name **NET311-Lab-07.imn**.

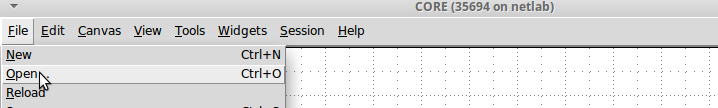


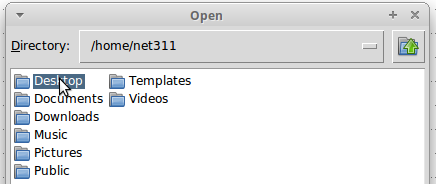
10. Run the CORE Network Emulator

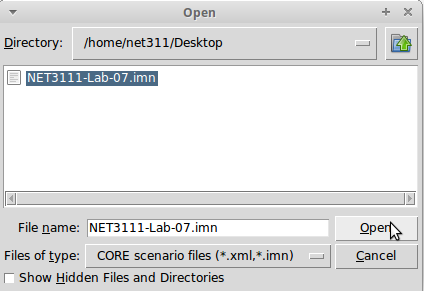




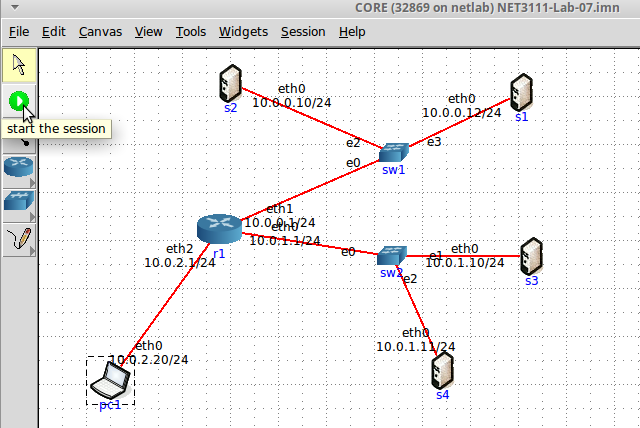
11. From the **File** menu, **open** the file **NET311-Lab-07.imn** from your Desktop folder.







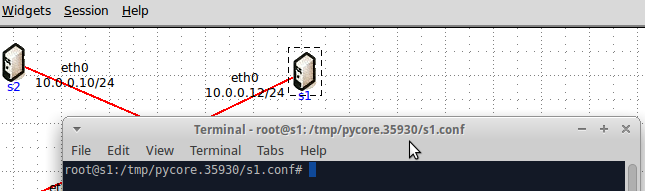
12. Click on the green button to start the session



## Lab sheet 1.1: provide a screenshot showing the running network session.

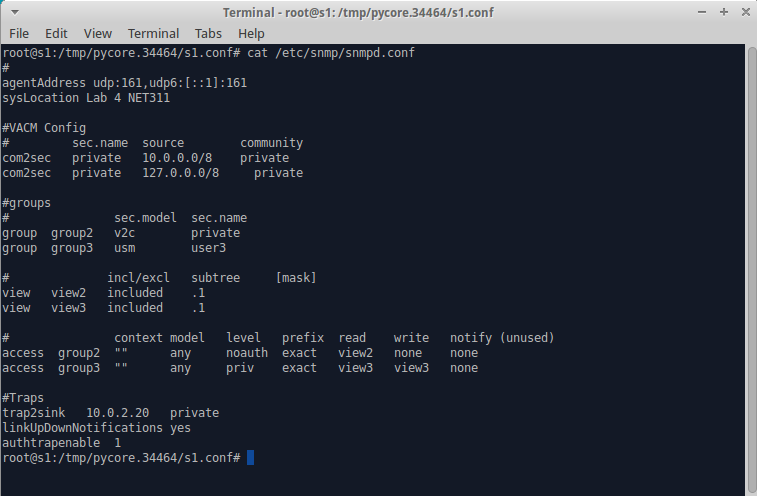
# Part 2: Analyze SNMPv2 Get-Request and Set-Request PDUs

1. Double-click on server **s1** to access its terminal.



2. Review the contents of the file **/etc/snmp/snmpd.conf** on **s1**.

cat /etc/snmp/snmpd.conf

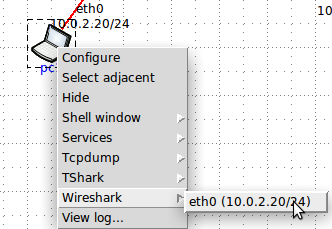


## Lab sheet 2.1: provide a screenshot showing the contents of the /etc/snmp/snmpd.conf file on s1.

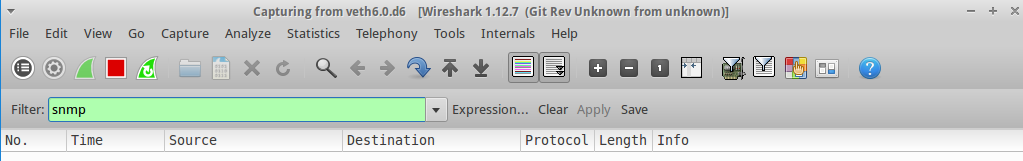
3. Review the contents of the file **/var/lib/snmp/snmpd.conf** on **s1**.

cat /var/lib/snmp/snmpd.conf

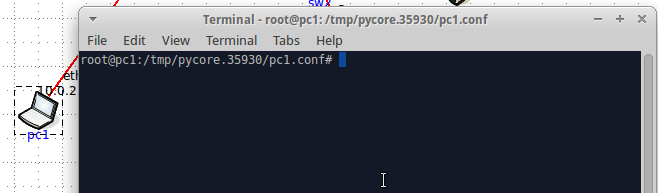
4. Right click on the host **pc1** to run **Wireshark** on the link **eth0**.



5. Enter snmp in the Filter input in Wireshark.

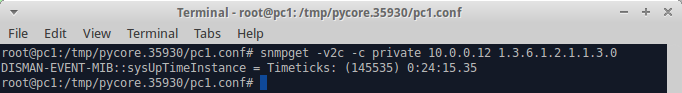


6. Double click on the host **pc1** to open its terminal.



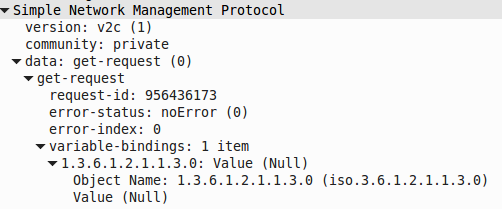
7. Send a get-request to host **s1** with a single OID (**sysUpTime**)

snmpget -v2c -c private 10.0.0.12 1.3.6.1.2.1.1.3.0



8. In Wireshark window, double click on the **get-request** line to inspect its contents



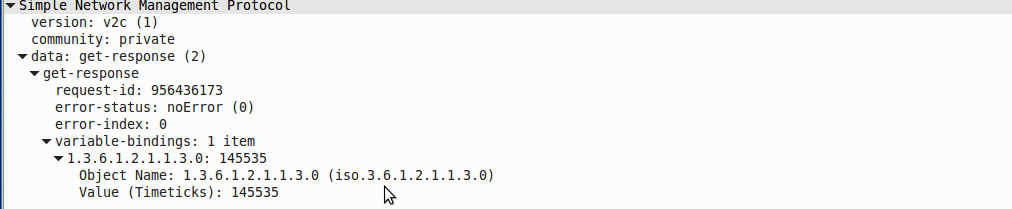


## Lab sheet 2.2: write the values of the PDU fields of the SNMP get-request as indicated in the table.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Application Header | Version | Community | PDU Type | Request ID | Error Status | Error Index | VarBind 1 name | VarBind 1 value |
| SNMP |  |  |  |  |  |  |  |  |

9. In Wireshark window, double click on the **get-response** line to inspect its contents





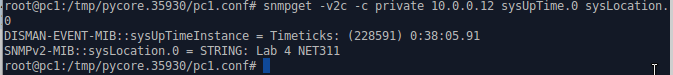
## Lab sheet 2.3: write the values of the PDU fields of the SNMP get-response as indicated in the table.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Application Header | Version | Community | PDU Type | Request ID | Error Status | Error Index | VarBind 1 name | VarBind 1 value |
| SNMP |  |  |  |  |  |  |  |  |

## Lab sheet 2.4: provide a screenshot showing the PDU fields of the SNMP get-response.

10. Send a **get-request** to host **s1** with a two OIDs (**sysUpTime, sysLocation**)

snmpget -v2c -c private 10.0.0.12 sysUpTime.0 sysLocation.0



11. In Wireshark window, double click on the **get-response** line to inspect its contents



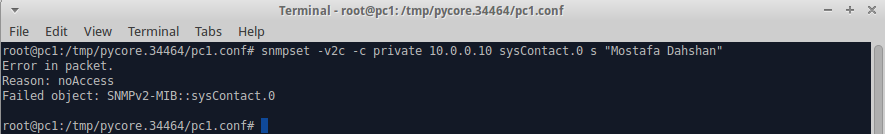
## Lab sheet 2.5: write the values of the PDU fields of the SNMP get-response as indicated in the table.

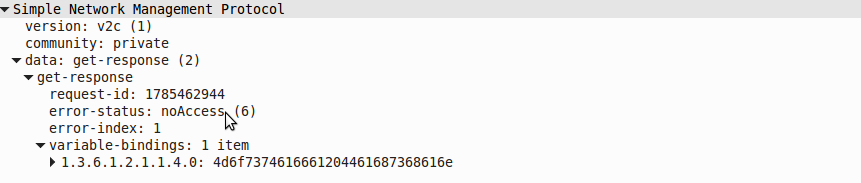
|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Application Header | Version | Community | PDU Type | Request ID | Error Status | Error Index | VarBind 1 name | VarBind 1 value | VarBind 2 name | VarBind 2 value |
| SNMP |  |  |  |  |  |  |  |  |  |  |

12. Send a **set-request** to host **s2** with one OID (**sysContact.0=Your Name**).

snmpset -v2c -c private 10.0.0.10 sysContact.0 s "Mostafa Dahshan"

Note that this requests results in an error, because community **private** only has read access to the subtree .1.





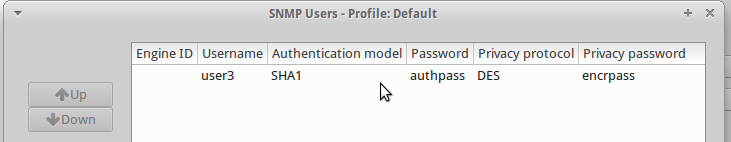
## Lab sheet 2.6: write the values of the PDU fields of the SNMP get-response as indicated in the table.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Application Header | Version | Community | PDU Type | Request ID | Error Status | Error Index | VarBind 1 name | VarBind 1 value |
| SNMP |  |  |  |  |  |  |  |  |

# Part 3: Analyze SNMPv2 GetBulk-Request and SNMPv3 Set-Request PDUs

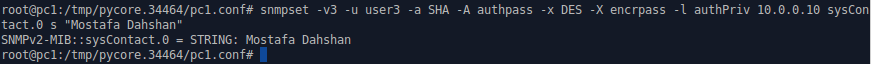
1. On Wireshark, go to **Edit** > **Preferences** > **Protocols** > **SNMP**. Click on **Users Table**.

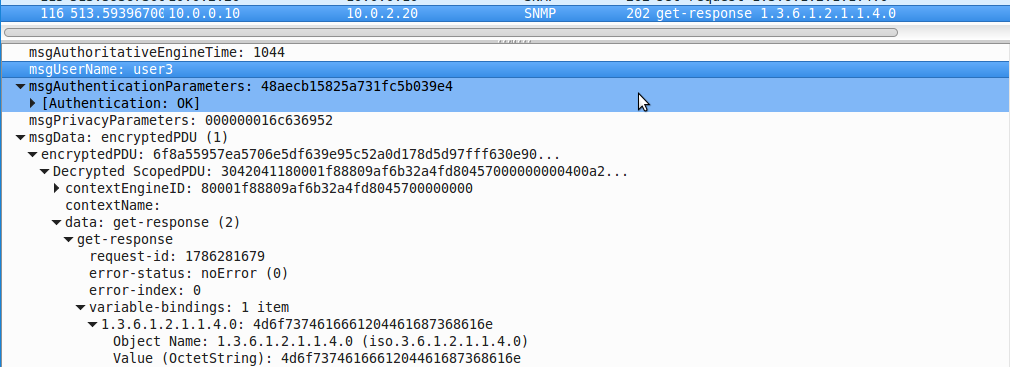
Configure the user **user3** with authentication password **authpass** and privacy password: **encrpass** for SNMP protocol.



2. Send a send-request to host **s2** with one OID (**sysContact.0=Your Name**), this time using SNMPv3 user **user3**.

snmpset -v3 -u user3 -a SHA -A authpass -x DES -X encrpass -l authPriv  
10.0.0.10 sysContact.0 s "Mostafa Dahshan"

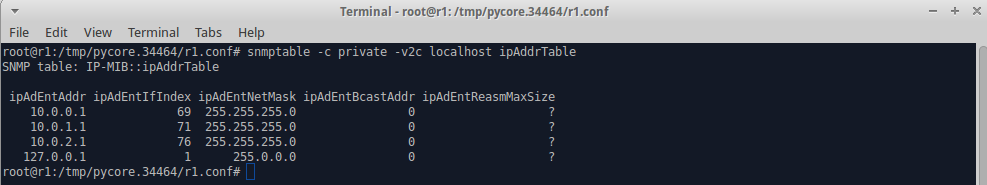




## Lab sheet 3.1: provide a screenshot showing the output of the response to the set-request in Wireshark.

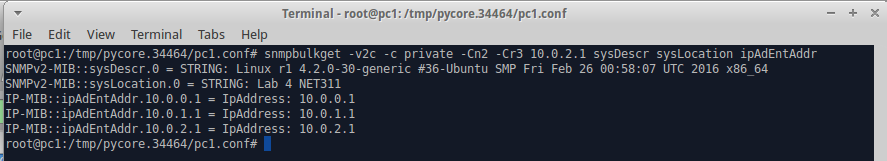
3. Double-click on router **r1**, then review the **ipAddrTable** using the following command:

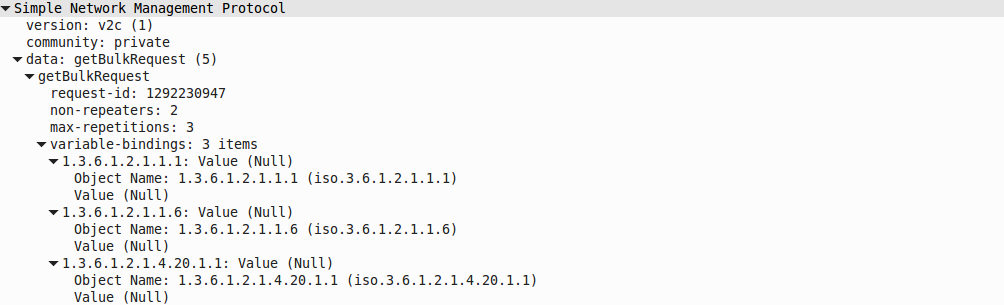
snmptable -c private -v2c localhost ipAddrTable



4. From **pc1**, send getbulk-request to r1 with **2** non-repetitive objects (**sysDescr**, **sysLocation**) and max-repetitions of **3** of the columnar object **ipAdEntAddr**.

snmpbulkget -v2c -c private -Cn2 -Cr3 10.0.2.1 sysDescr sysLocation ipAdEntAddr



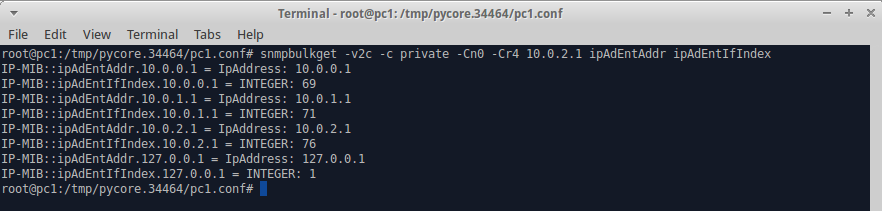


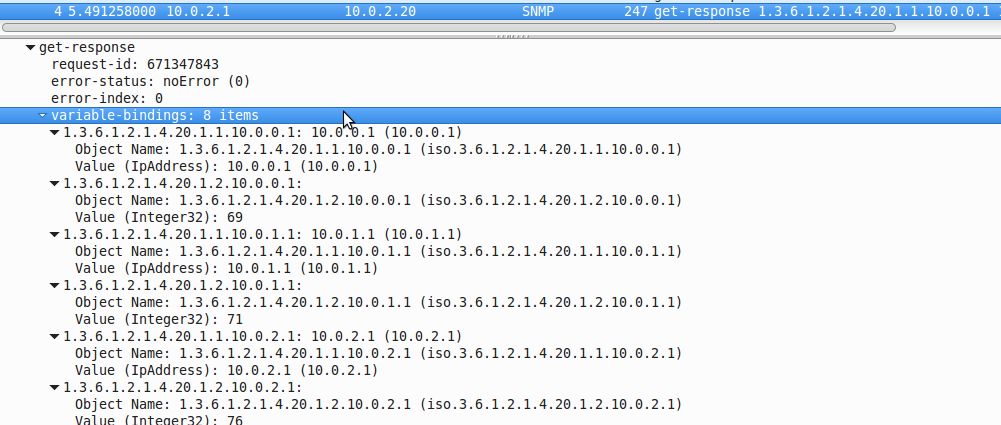
## Lab sheet 3.2: write the values of the PDU fields of the SNMP get-response as indicated in the table.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Version | Community | PDU Type | Request ID | Non-repeaters | Max-repetitions | VarBind 1 name | VarBind 1 value | … | VarBind 3 name | VarBind 3 value |
|  |  |  |  |  |  |  |  |  |  |  |

5. Send getbulk-request to r1 with **0** non-repetitive objects and max-repetitions of **4** of the two columns **ipAdEntAddr** and **ipAdEntIfIndex**.

snmpbulkget -v2c -c private -Cn0 -Cr4 10.0.2.1 ipAdEntAddr ipAdEntIfIndex



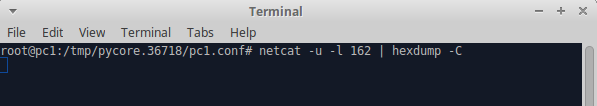


## Lab sheet 3.3: provide a screenshot showing the output of the response to the getbulk-request in Wireshark.

# Part 4: Analyze SNMPv2 Trap PDU

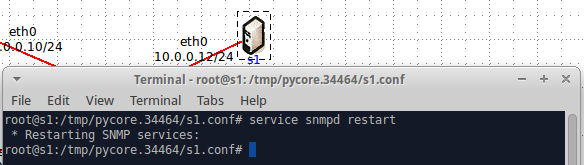
1. Double-click on host **pc1** to open a terminal, then write the following command to listen for snmp traps.

netcat -u -l 162 | hexdump -C

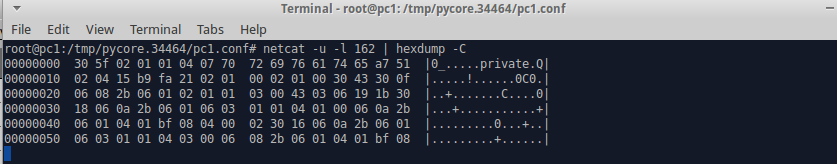


1. Double-click on host **s1** to open the terminal. Then write the following command to trigger a trap.

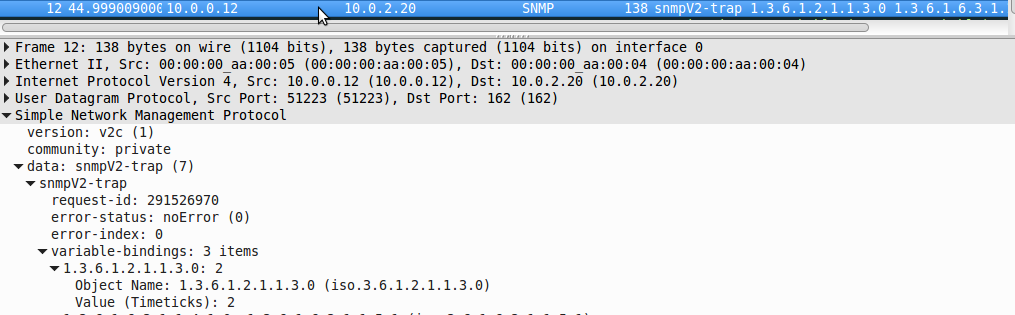
service snmpd restart



The output on pc1 should look like the following.



The captured packet on Wireshark should look like the following:



## Lab sheet 4.1: write the values of the PDU fields of the last SNMPv2 trap received by pc1.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | PDU Type | Request ID | Error Status | Error Index | VarBind 1 name | VarBind 1 value |
|  |  |  |  |  |  |  |