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

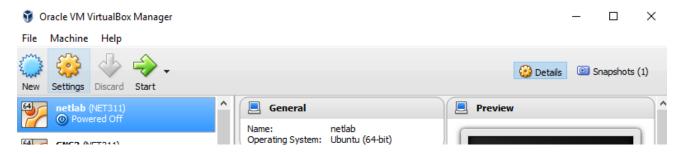
- 1. Using CORE Network Emulator GUI.
- 2. CORE Network Emulator: Video Tutorials.
- 3. CORE Network Emulator: Install Network Services.
- 4. Manpage of snmpd.conf Examples.
- 5. VACM: Net-snmp tutorials.
- 6. VACM (Access Control) configuration.
- 7. Manpage of snmpset.
- 8. Manpage of snmpbulkget.
- 9. <u>netcat Linuxintro</u>.

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

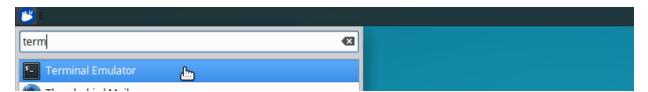
1. Start the netlab Linux virtual machine.



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

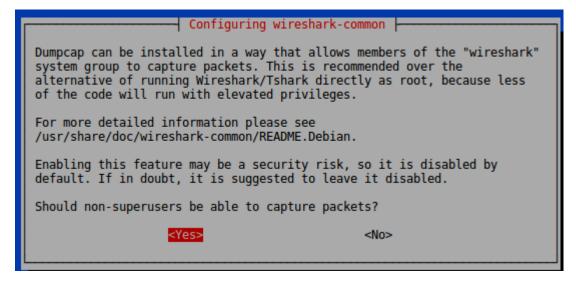


3. Run the Terminal emulator



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

sudo dpkg-reconfigure wireshark-common



5. Click Yes.

6. Run the following command

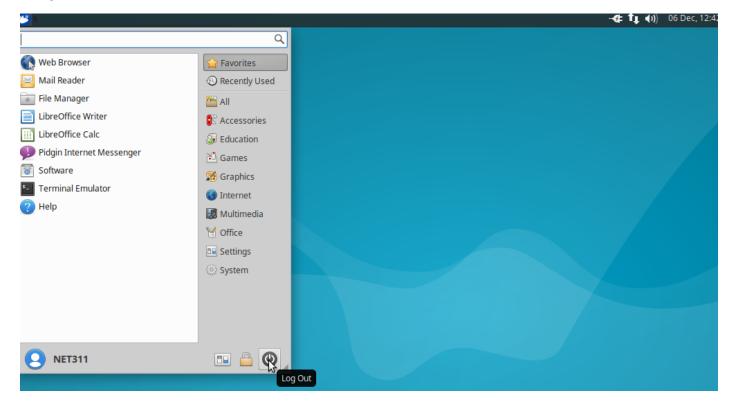
sudo usermod -a -G wireshark \$USER

```
Terminal - net311@netlab: ~ - + ×

File Edit View Terminal Tabs Help

net311@netlab: ~$ sudo dpkg-reconfigure wireshark-common
[sudo] password for net311:
net311@netlab: ~$ sudo usermod -a -G wireshark $USER
net311@netlab: ~$ ■
```

7. Log out.



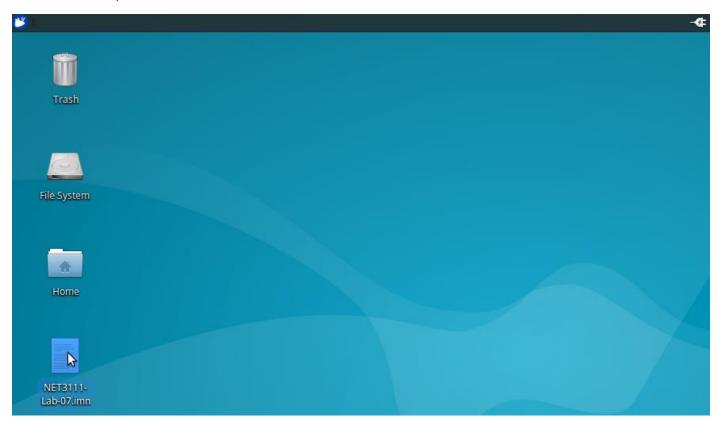


8. Log in again with the password: abc.311



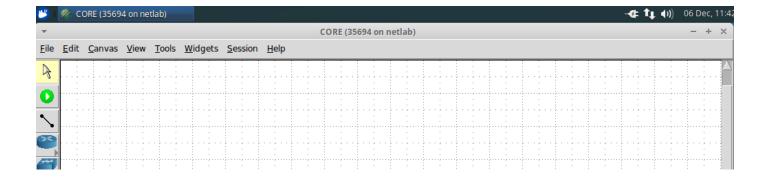
9. Locate the file **NET311-Lab-07.imn** included in the lab files. Copy the file to the desktop of the virtual machine.

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**.



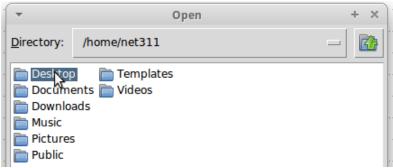
10. Run the CORE Network Emulator

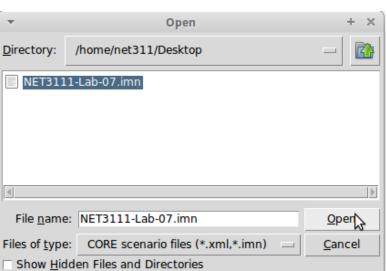




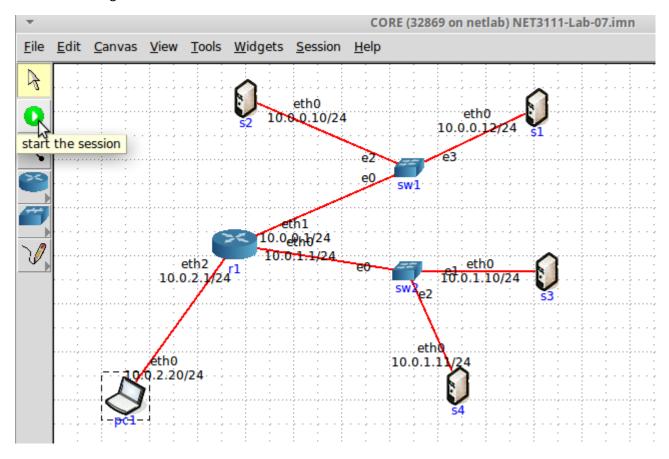
11. From the File menu, open the file NET311-Lab-07.imn from your Desktop folder.







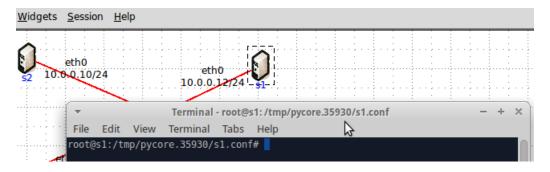
12. Click on the green button to start the session



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.

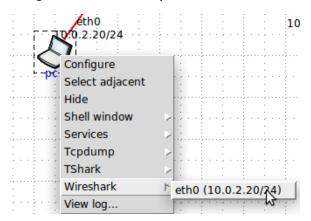
```
cat /etc/snmp/snmpd.conf
                                Terminal - root@s1: /tmp/pycore.34464/s1.conf
     Edit View Terminal Tabs Help
root@s1:/tmp/pycore.34464/s1.conf# cat /etc/snmp/snmpd.conf
agentAddress udp:161,udp6:[::1]:161
sysLocation Lab 4 NET311
#VACM Config
          sec.name source
                                   community
                    10.0.0.0/8
com2sec
                                   private
          private
com2sec
          private
                    127.0.0.0/8
                                    private
#groups
                sec.model
                           sec.name
       group2
                v2c
                           private
group
group
       group3
                usm
                           user3
               incl/excl
                           subtree
                                        [mask]
view
       view2
               included
               included
view
       view3
                            .1
                                 level
                                         prefix
                                                                 notify (unused)
                context model
                                                 read
                                                         write
                                 noauth exact
        group2
                                                 view2
                                                         none
                                                                 none
                        any
access
        group3
                        any
                                 priv
                                         exact
                                                 view3
                                                         view3
                                                                 none
#Traps
trap2sink
            10.0.2.20
                        private
linkUpDownNotifications yes
authtrapenable 1
root@s1:/tmp/pycore.34464/s1.conf#
```

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

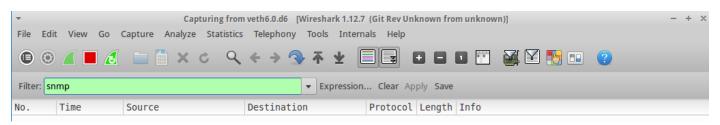
3. Review the contents of the file /var/lib/snmp/snmpd.conf on s1.

```
cat /var/lib/snmp/snmpd.conf
```

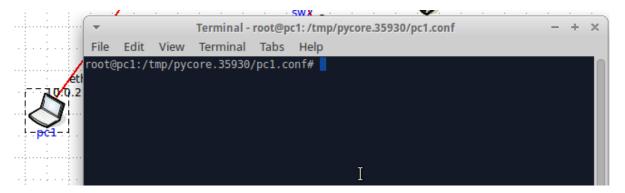
4. Right click on the host pc1 to run Wireshark on the link eth0.



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)

Terminal Tabs Help

File

Edit

View

root@pc1:/tmp/pycore.35930/pc1.conf# snmpget -v2c -c private 10.0.0.12 1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (145535) 0:24:15.35
root@pc1:/tmp/pycore.35930/pc1.conf#

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

No.	Time	Source	Destination		Protocol	Length	Info
	3 4.310976000	10.0.2.20	10.0.0.12		SNMP	86	get-request 1.3.6.1.2.1.1.3.0
	4 4.311793000	10.0.0.12	10.0.2.20 W	3	SNMP	89	get-response 1.3.6.1.2.1.1.3.0

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

Application	Version	Community	PDU	Request	Error	Error	VarBind 1	VarBind 1
Header			Туре	ID	Status	Index	name	value
SNMP								

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

No.	Time	Source		Destination		Protocol	Length	Info		
	3 4.310976000	10.0.2.20		10.0.0.12		SNMP	86	get-request	1.3.6.1.2.1.	1.3.0
	4 4.311793000	10.0.0.12	7	10.0.2.20		SNMP	89	get-response	1.3.6.1.2.1	.1.3.0
			W							
▼ Sim	ole Network Man	agement Protoco	ol							
	rsion: v2c (1)									
	mmunity: priva									
	ta: get-respons	se (2)								
▼!	get-response									
	request-id: 9									
	error-status:									
	error-index:									
٠ ا	rvariable-bind:	ings: 1 item								
	▼ 1.3.6.1.2.1.	1.3.0: 145535								
		e: 1.3.6.1.2.1.		so.3.6.1.2.1.1	.3.0)					
	Value (Time	eticks): 145535		₽						

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

Application	Version	Community	PDU	Request	Error	Error	VarBind 1	VarBind 1
Header			Type	ID	Status	Index	name	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)

root@pc1:/tmp/pycore.35930/pc1.conf#

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

root@pc1:/tmp/pycore.35930/pc1.conf# snmpget -v2c -c private 10.0.0.12 sysUpTime.0 sysLocation.
0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (228591) 0:38:05.91
SNMPv2-MIB::sysLocation.0 = STRING: Lab 4 NET311
```

176 834.87751100 10.0.0.12 10.0.2.20 SNMP 115 get-response 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.6

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

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

```
Terminal - root@pc1: /tmp/pycore.34464/pc1.conf
 File Edit View Terminal Tabs Help
root@pcl:/tmp/pycore.34464/pcl.conf# snmpset -v2c -c private 10.0.0.10 sysContact.0 s "Mostafa Dahshan'
Error in packet.
Reason: noAccess
Failed object: SNMPv2-MIB::sysContact.0
root@pc1:/tmp/pycore.34464/pc1.conf#
▼ Simple Network Management Protocol
   version: v2c (1)
   community: private

▼ data: get-response (2)

   request-id: 1785462944
      error-status: noAccess (6)
      error-index: 1
     ▼variable-bindings: 1 item
      ▶ 1.3.6.1.2.1.1.4.0: 4d6f7374616661204461687368616e
```

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

Application	Version	Community	PDU	Request	Error	Error	VarBind 1	VarBind 1
Header			Type	ID	Status	Index	name	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"
```

```
root@pcl:/tmp/pycore.34464/pcl.conf# snmpset -v3 -u user3 -a SHA -A authpass -x DES -X encrpass -l authPriv 10.0.0.10 sysContact.0 s "Mostafa Dahshan"
SNMPv2-MIB::sysContact.0 = STRING: Mostafa Dahshan
root@pcl:/tmp/pycore.34464/pcl.conf#
```

```
116 513.59396700 10.0.0.10
                                          10.0.2.20
                                                                              202 get-response 1.3.6.1.2.1.1.4.0
 msgAuthoritativeEngineTime: 1044
▼ msgAuthenticationParameters: 48aecb15825a731fc5b039e4
                                                                               1
 ▶ [Authentication: OK]
 msgPrivacyParameters: 000000016c636952
▼ msgData: encryptedPDU (1)
 ▼ encryptedPDU: 6f8a55957ea5706e5df639e95c52a0d178d5d97fff630e90...
  ▼ Decrypted ScopedPDU: 3042041180001f88809af6b32a4fd80457000000000400a2...
    ▶ contextEngineID: 80001f88809af6b32a4fd8045700000000
     contextName:
    ▼ data: get-response (2)

▼ get-response

        request-id: 1786281679
         error-status: noError (0)
         error-index: 0
       ▼variable-bindings: 1 item
         ▼1.3.6.1.2.1.1.4.0: 4d6f7374616661204461687368616e
            Object Name: 1.3.6.1.2.1.1.4.0 (iso.3.6.1.2.1.1.4.0)
            Value (OctetString): 4d6f7374616661204461687368616e
```

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

```
Terminal - root@r1:/tmp/pycore.34464/r1.conf — + ×

File Edit View Terminal Tabs Help

root@r1:/tmp/pycore.34464/r1.conf# snmptable -c private -v2c localhost ipAddrTable

SNMP table: IP-MIB::ipAddrTable

ipAdEntAddr ipAdEntIfIndex ipAdEntNetMask ipAdEntBcastAddr ipAdEntReasmMaxSize

10.0.0.1 69 255.255.255.0 0 ?

10.0.1.1 71 255.255.255.0 0 ?

10.0.2.1 76 255.255.255.0 0 ?

127.0.0.1 1 255.0.0.0 0 ?

root@r1:/tmp/pycore.34464/r1.conf#
```

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

```
Terminal - root@pc1:/tmp/pycore.34464/pc1.conf - + ×

File Edit View Terminal Tabs Help

root@pc1:/tmp/pycore.34464/pc1.conf# snmpbulkget -v2c -c private -Cn2 -Cr3 10.0.2.1 sysDescr sysLocation ipAdEntAddr

SNMPv2-MIB::sysDescr.0 = STRING: Linux r1 4.2.0-30-generic #36-Ubuntu SMP Fri Feb 26 00:58:07 UTC 2016 x86_64

SNMPv2-MIB::sysLocation.0 = STRING: Lab 4 NET311

IP-MIB::ipAdEntAddr.10.0.0.1 = IpAddress: 10.0.0.1

IP-MIB::ipAdEntAddr.10.0.1.1 = IpAddress: 10.0.1.1

IP-MIB::ipAdEntAddr.10.0.2.1 = IpAddress: 10.0.2.1

root@pc1:/tmp/pycore.34464/pc1.conf#
```

```
▼ Simple Network Management Protocol
   version: v2c (1)
   community: private

▼ data: getBulkRequest (5)

▼ getBulkRequest

      request-id: 1292230947
      non-repeaters: 2
      max-repetitions: 3
    ▼ variable-bindings: 3 items
      ▼1.3.6.1.2.1.1.1: Value (Null)
         Object Name: 1.3.6.1.2.1.1.1 (iso.3.6.1.2.1.1.1)
         Value (Null)
      ▼1.3.6.1.2.1.1.6: Value (Null)
         Object Name: 1.3.6.1.2.1.1.6 (iso.3.6.1.2.1.1.6)
         Value (Null)
      ▼1.3.6.1.2.1.4.20.1.1: Value (Null)
         Object Name: 1.3.6.1.2.1.4.20.1.1 (iso.3.6.1.2.1.4.20.1.1)
         Value (Null)
```

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

٧	ersion	Community	PDU	Request	Non-	Max-	VarBind	VarBind	 VarBind	VarBind
			Type	ID	repeaters	repetitions	1 name	1 value	3 name	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

```
▼ get-response
  request-id: 671347843
  error-status: noError (0)
  error-index: 0
  variable-bindin
  ▼1.3.6.1.2.1.4.20.1.1.10.0.0.1: 10.0.0.1 (10.0.0.1)
     Object Name: 1.3.6.1.2.1.4.20.1.1.10.0.0.1 (iso.3.6.1.2.1.4.20.1.1.10.0.0.1)
     Value (IpAddress): 10.0.0.1 (10.0.0.1)
  ▼1.3.6.1.2.1.4.20.1.2.10.0.0.1:
     Object Name: 1.3.6.1.2.1.4.20.1.2.10.0.0.1 (iso.3.6.1.2.1.4.20.1.2.10.0.0.1)
     Value (Integer32): 69
  ▼1.3.6.1.2.1.4.20.1.1.10.0.1.1: 10.0.1.1 (10.0.1.1)
     Object Name: 1.3.6.1.2.1.4.20.1.1.10.0.1.1 (iso.3.6.1.2.1.4.20.1.1.10.0.1.1)
     Value (IpAddress): 10.0.1.1 (10.0.1.1)
  ▼1.3.6.1.2.1.4.20.1.2.10.0.1.1:
     Object Name: 1.3.6.1.2.1.4.20.1.2.10.0.1.1 (iso.3.6.1.2.1.4.20.1.2.10.0.1.1)
     Value (Integer32): 71
  ▼1.3.6.1.2.1.4.20.1.1.10.0.2.1: 10.0.2.1 (10.0.2.1)
     Object Name: 1.3.6.1.2.1.4.20.1.1.10.0.2.1 (iso.3.6.1.2.1.4.20.1.1.10.0.2.1)
     Value (IpAddress): 10.0.2.1 (10.0.2.1)
  ▼1.3.6.1.2.1.4.20.1.2.10.0.2.1:
     Object Name: 1.3.6.1.2.1.4.20.1.2.10.0.2.1 (iso.3.6.1.2.1.4.20.1.2.10.0.2.1)
     Value (Integer32): 76
```

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 ▼ Terminal - + × File Edit View Terminal Tabs Help root@pcl:/tmp/pycore.36718/pcl.conf# 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.

```
eth0
.6.0.10/24

Terminal - root@s1:/tmp/pycore.34464/s1.conf
File Edit View Terminal Tabs Help
root@s1:/tmp/pycore.34464/s1.conf# service snmpd restart
* Restarting SNMP services:
root@s1:/tmp/pycore.34464/s1.conf#
```

The output on pc1 should look like the following.

```
Terminal - root@pc1: /tmp/pycore.34464/pc1.conf
File
     Edit
          View Terminal
                                 Help
                           Tabs
oot@pc1:/tmp/pycore.34464/pc1.conf# netcat
00000000 30 5f 02 01 01 04 07 70
                                   72 69 76 61 74 65 a7 51
                                                                     .private.0
         02 04 15 b9 fa 21 02 01
00000010
                                   00 02 01 00 30 43 30 0f
00000020
         06 08 2b 06 01 02 01 01
                                   03 00
                                         43 03 06
                                                      1b 30
00000030
         18 06 0a 2b 06 01 06 03
                                   01 01 04 01 00 06 0a 2b
         06 01 04 01 bf 08 04 00
                                   02 30 16 06 0a 2b 06 01
00000040
00000050
         06 03 01 01 04 03 00 06
                                   08 2b 06 01 04 01
                                                     bf 08
```

The captured packet on Wireshark should look like the following:

```
▶ Frame 12: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
▶ Ethernet II, Src: 00:00:00_aa:00:05 (00:00:00:aa:00:05), Dst: 00:00:00_aa:00:04 (00:00:00:aa:00:04)
▶ Internet Protocol Version 4, Src: 10.0.0.12 (10.0.0.12), Dst: 10.0.2.20 (10.0.2.20)
▶ User Datagram Protocol, Src Port: 51223 (51223), Dst Port: 162 (162)
▼ Simple Network Management Protocol
   version: v2c (1)
   community: private
 ▼ data: snmpV2-trap (7)

▼ snmpV2-trap

      request-id: 291526970
      error-status: noError (0)
      error-index: 0

▼ variable-bindings: 3 items

      ▼1.3.6.1.2.1.1.3.0: 2
         Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
         Value (Timeticks): 2
```

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