LAB EXPERIMENT: MIB II and SNMP Analysis

Questions

1) Which Transport Protocol and Ports are used for SNMP Protocol ?

UDP, Ports: 161 and 162

2) How are the community strings sent: encrypted or not encrypted?

not encrypted

3) How many reply messages did you capture during the first *SNMP Walk* example? Explain your answer.

Many, SNMP Walk is using SNMP GetNext request in a recursive way.

4) Briefly explain the difference between *SNMP Get* and *SNMP GetNext* request.

SNMP Get requests object specified by OID
SNMP GetNext request object that is next to specified one.
SNMP GetNext request can contain also uncompleted OID

5) Explain: which layer is the SNMP Protocol placed at?

Application Layer

6) Explain: when does an Agent send a TRAP to the Manager?

When the administrator had set trap (or threshold) for event, and this event occurs.

7) Indicate the main differences between SNMPv2 and SNMPv3.

SNMPv3 supports in addition to SNMPv2:
secure authentication, encryption, view access control model

8) What are the main differences between MIB II and RMON-MIB ?

RMON-MIB extends the functionality of MIB II, it contains advanced monitoring information for LAN Networking.

9) Consider the following SNMP message which was captured using Wireshark analyzer.
Which Object was requested and which value was returned?
Explain your answer.

Frame 2 (84 bytes on wire, 84 bytes captured)
Ethernet II, Src: 00:11:92:83:49:20, Dst: 00:06:5b:75:c1:fe
Internet Protocol, Src. Addr: 194.95.109.130 (194.95.109.130), Dst. Addr: 194.95.109.181 (194.95.109.181)
User Datagram Protocol, Src Port: **snmp** (161), Dst Port: 1276 (1276)
Simple Network Management Protocol
Version: 1 (0)
Community: public
PDU type: RESPONSE (2)
Request Id: 0x00000004
Error Status: NO ERROR (0)
Error Index: 0
Object identifier : ??????????????????????????????????
Value: Counter32: ??????????????????

0000 00 06 5b 75 c1 fe 00 11 92 83 49 20 08 00 45 00 ..[u.....I ..E.
0010 00 46 90 20 00 00 ff 11 cb 8f c2 5f 6d 82 c2 5f .F. ....._m.._
0020 6d b5 00 a1 04 fc 00 32 08 82 30 28 02 01 00 04 m......2..0(....
0030 06 70 75 62 6c 69 63 a2 1b 02 01 04 02 01 00 02 .public.....
0040 30 0e **06 08 2b 06 01 02 01 04 04 00 41 02 1c 2b** **……..**

Answer: OID 1.3.6.1.2.1.4.4.0 Type 0x41 Counter Len 2 Bytes Value: 7211

Explanation: ipInHdrErrors has value 7211

10) Consider the SNMP Listing No. 1 and 2.
The "Labserver" host from the Laboratory was queried using an SNMP browser.

10.1. Please identify what kind of interfaces are connected to the Labserver?

IF_Index: 1 has Type 24 : Loopback
IF_Index: 16777219 - 16777221: Type 6: Ethernet (CSMA/CD)

10.2. Please identify what kind of IP addresses are assigned to these interfaces?

IF 16777219 has : 192.168.0.140; 192.168.10.140; 192.168.20.140; 192.168.30.140
IF 16777220 has : 194.95.109.66; 194.95.109.82
IF 16777221 has : 194.95.109.140

Listing 1

C:\>snmputil walk labserver public 1.3.6.1.2.1.4.20.1.2

```
Variable = ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex.127.0.0.1
Value = INTEGER - 1
Variable = ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex.192.168.0.140
Value = INTEGER - 16777219
Variable = ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex.192.168.10.140
Value = INTEGER - 16777219
Variable = ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex.192.168.20.140
Value = INTEGER - 16777219
Variable = ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex.192.168.30.140
Value = INTEGER - 16777219
Variable = ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex.194.95.109.66
Value = INTEGER - 16777220
Variable = ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex.194.95.109.82
Value = INTEGER - 16777220
Variable = ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex.194.95.109.140
Value = INTEGER - 16777221
End of MIB subtree.
```

C:\>snmputil walk labserver public 1.3.6.1.2.1.2.2.1.2

```
Variable = interfaces.ifTable.ifEntry.ifDescr.1
Value = OCTET STRING - MS TCP Loopback interface<0x0>
Variable = interfaces.ifTable.ifEntry.ifDescr.16777219
Value = OCTET STRING - Intel(R) PRO/100+ Server Adapter (PILA8470B)<0x0>
Variable = interfaces.ifTable.ifEntry.ifDescr.16777220
Value = OCTET STRING - Intel(R) PRO/100+ Server Adapter (PILA8470B)<0x0
Variable = interfaces.ifTable.ifEntry.ifDescr.16777221
Value = OCTET STRING - Intel(R) PRO/100 Network Connection<0x0>
End of MIB subtree.
```

Listing 2

C:\>snmputil walk labserver public 1.3.6.1.2.1.2.2.1.3

```
Variable = interfaces.ifTable.ifEntry.ifType.1
Value = INTEGER - 24
Variable = interfaces.ifTable.ifEntry.ifType.16777219
Value = INTEGER - 6
Variable = interfaces.ifTable.ifEntry.ifType.16777220
Value = INTEGER - 6
Variable = interfaces.ifTable.ifEntry.ifType.16777221
Value = INTEGER - 6
End of MIB subtree.
```

C:\>snmputil walk labserver public 1.3.6.1.2.1.2.2.1.5

```
Variable = interfaces.ifTable.ifEntry.ifSpeed.1
Value = Guage - 10000000
Variable = interfaces.ifTable.ifEntry.ifSpeed.16777219
Value = Guage - 100000000
Variable = interfaces.ifTable.ifEntry.ifSpeed.16777220
Value = Guage - 10000000
Variable = interfaces.ifTable.ifEntry.ifSpeed.16777221
Value = Guage - 100000000
End of MIB subtree.
```