Assignment 5 - Wireshark Lab: UDP v6.1

Packet trace taken from author

Answer 1:

```
     1 2003-09-23 05:39:52.896793 192.168.1.102         192.168.1.104         SNMP     92     get-request 1.3.6
.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: DellComp 4f:36:23 (00:08:74:4f:36:23), Dst: Hewlett- 61:eb:ed (00:30:c1:61:eb:ed)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 192.168.1.104 (192.168.1.104)
User Datagram Protocol, Src Port: 4334 (4334), Dst Port: 161 (161)
  Source Port: 4334 (4334)
  Destination Port: 161 (161)
  Length: 58
  Checksum: 0x65f8 [validation disabled]
  [Stream index: 0]
Simple Network Management Protocol
```

- The number of fields in the UDP Header is 4. They are –
  - Source Port
  - Destination Port
  - Length
  - Checksum

Answer 2:

```
  Source Port: 4334 (4334)
  Destination Port: 161 (161)
  Length: 58
  Checksum: 0x65f8 [validation disabled]
  [Stream index: 0]
Simple Network Management Protocol

0000  00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00   .0.a....tO6#..E.
0010  00 4e 02 fd 00 00 80 11 00 00 c0 a8 01 66 c0 a8   .N...........f..
0020  01 68 10 ee 00 a1 00 3a 65 f8 30 30 02 01 00 04   .h.....:e.00....
0030  06 70 75 62 6c 69 63 a0 23 02 02 18 fb 02 01 00   .public.#.......
0040  02 01 00 30 17 30 15 06 11 2b 06 01 04 01 0b 02   ...0.0...+......
0050  03 09 04 02 01 02 02 02 01 00 05 00               ............
```

Hex	Decimal	Field	Size
10 ee	4334	Source Port	2 Bytes
00 a1	161	Destination Port	2 Bytes
00 3a	58	Length	2 Bytes
65 f8	Not required	Checksum	2 Bytes

- Size of each of the UDP Header fields is 2 Bytes.
- Also it means UDP header can have maximum of 2 * 4(fields) =8 Bytes size.

Answer 3:

```
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: DellComp 4f:36:23 (00:08:74:4f:36:23), Dst: Hewlett- 61:eb:ed (00:30:c1:61:eb:ed)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 192.168.1.104 (192.168.1.104)
User Datagram Protocol, Src Port: 4334 (4334), Dst Port: 161 (161)
  Source Port: 4334 (4334)
  Destination Port: 161 (161)
  Length: 58
  Checksum: 0x65f8 [validation disabled]
  [Stream index: 0]
Simple Network Management Protocol

0000  00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00   .0.a....tO6#..E.
0010  00 4e 02 fd 00 00 80 11 00 00 c0 a8 01 66 c0 a8   .N...........f..
0020  01 68 10 ee 00 a1 00 3a 65 f8 30 30 02 01 00 04   .h.....:e.00....
0030  06 70 75 62 6c 69 63 a0 23 02 02 18 fb 02 01 00   .public.#.......
0040  02 01 00 30 17 30 15 06 11 2b 06 01 04 01 0b 02   ...0.0...+......
0050  03 09 04 02 01 02 02 02 01 00 05 00               ............
```

- The value in the Length Field is = 58 and it's the Size of UDP that includes Header and data. Since we know from 2nd answer that header fields are only 8 bytes so this value can only represent the size of the entire packet including header.

Answer 4:

- The maximum size that can be included in the UDP payload depends on the maximum value the 16bit integer field (**= Length**) can hold. The maximum value of 2^16 -1 (=**65535**).
  - Header = 2 Bytes * 4(fields) = 8 Bytes
  - Total = 65535 Bytes
  - Pay Load Size = Total – header = 65535 – 8 = **65527**

Answer 5:

- The largest possible source port number is again the maximum value of 2^16 – 1 (=**65535**)

Answer 6:

```
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: DellComp 4f:36:23 (00:08:74:4f:36:23), Dst: Hewlett- 61:eb:ed (00:30:c1:61:eb:ed)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 192.168.1.104 (192.168.1.104)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 78
  Identification: 0x02fd (765)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 128
  Protocol: UDP (17)
  Header checksum: 0x0000 [validation disabled]
```

- The protocol number of UDP is **17 in decimal and 0x11 in hex.**

Answer 7:

```
No.     Time                        Source                Destination           Protocol Length Info
      1 2003-09-23 05:39:52.896793 192.168.1.102         192.168.1.104         SNMP     92     get-request 1.3.6
.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: DellComp 4f:36:23 (00:08:74:4f:36:23), Dst: Hewlett- 61:eb:ed (00:30:c1:61:eb:ed)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 192.168.1.104 (192.168.1.104)
User Datagram Protocol, Src Port: 4334 (4334), Dst Port: 161 (161)
Simple Network Management Protocol
```

First Packet

```
No.     Time                        Source                Destination           Protocol Length Info
      2 2003-09-23 05:39:52.913753 192.168.1.104         192.168.1.102         SNMP     93     get-response 1.3.
6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

Frame 2: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
Ethernet II, Src: Hewlett- 61:eb:ed (00:30:c1:61:eb:ed), Dst: DellComp 4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 192.168.1.104 (192.168.1.104), Dst: 192.168.1.102 (192.168.1.102)
User Datagram Protocol, Src Port: 161 (161), Dst Port: 4334 (4334)
Simple Network Management Protocol
```

Second Packet

- The first packet is a UDP packet sent from Source Address : - **192.168.1.102** to Destination Address :- **192.168.1.104**
- The second packet is a UDP response packet from Source Address : - **192.168.1.104** to Destination Address :- **192.168.1.102**
- The port numbers in the two packets indicate that there is a transfer of messages using UDP Protocol between two applications using SNMP Application layer protocol in the same network.
- One application at **192.168.1.102** is listening at **port 4334** and other application at **192.168.1.104** is listening at **port 161**