



COMPUTER NETWORKS LAB

ROLL NO: 19P0012
NAME: AITZAZ TAHIR CH
SECTION: BS(CS)-5B
LAB NO: 5 UDP



Q1:

There are 4 Fields in UDP header:

- Source Port
- Destination Port
- Length
- Checksum

```
Wireshark · Packet 13 · Wi-Fi
> Frame 13: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{6C95DF2E-7C0F-4763-8F77-C9A70E9C6508}, id 0
> Ethernet II, Src: zte_de:b8:c8 (24:d3:f2:de:b8:c8), Dst: IntelCor_eb:35:c5 (08:71:90:eb:35:c5)
> Internet Protocol Version 4, Src: 142.250.181.106, Dst: 192.168.1.20
> User Datagram Protocol, Src Port: 443, Dst Port: 55828
  Source Port: 443
  Destination Port: 55828
  Length: 33
  Checksum: 0xa819 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
  > [Timestamps]
  UDP payload (25 bytes)
> Data (25 bytes)

0000  08 71 90 eb 35 c5 24 d3 f2 de b8 c8 08 00 45 80  .q--5-$- .....E-
0010  00 35 00 00 40 00 39 11 3b 17 8e fa b5 6a c0 a8  .5--@.9- ;....j..
0020  01 14 01 bb da 14 00 21 a8 19 4e 97 d9 e6 d1 10  ..-...!..N.....
0030  91 ee 65 0c 8f 7f 2c f4 07 fa 3f 26 3d f3 cf 8c  ..e...,-...?&=...
0040  d8 02 9c                                     ...
```

Q2:

UDP header is 16 hexadecimal characters long; 16 hex = 64 bits = 8 bytes.

- Source Port (16bit or 8bytes)
- Destination Port (16bit or 8bytes)
- Length (16bit or 8bytes)
- Checksum (16bit or 8bytes)

```
Wireshark · Packet 13 · Wi-Fi
> Frame 13: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{6C95DF2E-7C0F-4763-8F77-C9A70E9C6508}, id 0
> Ethernet II, Src: zte_de:b8:c8 (24:d3:f2:de:b8:c8), Dst: IntelCor_eb:35:c5 (08:71:90:eb:35:c5)
> Internet Protocol Version 4, Src: 142.250.181.106, Dst: 192.168.1.20
> User Datagram Protocol, Src Port: 443, Dst Port: 55828
  Source Port: 443
  Destination Port: 55828
  Length: 33
  Checksum: 0xa819 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
  > [Timestamps]
  UDP payload (25 bytes)
> Data (25 bytes)

0000  08 71 90 eb 35 c5 24 d3 f2 de b8 c8 08 00 45 80  .q--5-$- .....E-
0010  00 35 00 00 40 00 39 11 3b 17 8e fa b5 6a c0 a8  .5--@.9- ;....j..
0020  01 14 01 bb da 14 00 21 a8 19 4e 97 d9 e6 d1 10  ..-...!..N.....
0030  91 ee 65 0c 8f 7f 2c f4 07 fa 3f 26 3d f3 cf 8c  ..e...,-...?&=...
0040  d8 02 9c                                     ...
```

Q3:

Length field shows the size of the entire segment “header+payload”. We do not need to specify header length separately because all UDP headers are of the same size.

In my packet length = 33

So, payload => 33 - 8 = 25 bytes

Header = 8 bytes

```
Wireshark · Packet 13 · Wi-Fi

> Frame 13: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{6C95DF2E-7C0F-4763-8F77-C9A70E9C6508}, id 0
> Ethernet II, Src: zte_de:b8:c8 (24:d3:f2:de:b8:c8), Dst: IntelCor_eb:35:c5 (08:71:90:eb:35:c5)
> Internet Protocol Version 4, Src: 142.250.181.106, Dst: 192.168.1.20
▼ User Datagram Protocol, Src Port: 443, Dst Port: 55828
  Source Port: 443
  Destination Port: 55828
  Length: 33
  Checksum: 0xa819 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
  > [Timestamps]
  UDP payload (25 bytes)
> Data (25 bytes)

0000  08 71 90 eb 35 c5 24 d3 f2 de b8 c8 08 00 45 80  -q--5-$- .....E-
0010  00 35 00 00 40 00 39 11 3b 17 8e fa b5 6a c0 a8  -5--@-9- ;....j..
0020  01 14 01 bb da 14 00 21 a8 19 4e 97 d9 e6 d1 10  -.....!-N-----
0030  91 ee 65 0c 8f 7f 2c f4 07 fa 3f 26 3d f3 cf 8c  --e---,--?&=---
0040  d8 02 9c                                     ...
```

Q4:

Maximum size of UDP payload is $(2^{16})-1$, We also need to deduct extra 8 bytes for the header.

So, the maximum size of the payload can be 65527 bytes.

Q5:

Largest possible port number is $(2^{16})-1$ => 65535 bytes.

Q6:

Protocol number for UDP is 11 in hexadecimal or 17 in decimal.

```
Wireshark · Packet 13 · Wi-Fi

> Frame 13: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{6C95DF2E-7C0F-4763-8F77-C9A70E9C6508}, id 0
> Ethernet II, Src: zte_de:b8:c8 (24:d3:f2:de:b8:c8), Dst: IntelCor_eb:35:c5 (08:71:90:eb:35:c5)
▼ Internet Protocol Version 4, Src: 142.250.181.106, Dst: 192.168.1.20
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x80 (DSCP: CS4, ECN: Not-ECT)
  Total Length: 53
  Identification: 0x0000 (0)
  > Flags: 0x40, Don't fragment
  Fragment Offset: 0
  Time to Live: 57
  Protocol: UDP (17)
  Header Checksum: 0x3b17 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 142.250.181.106

0000  08 71 90 eb 35 c5 24 d3 f2 de b8 c8 08 00 45 80  -q--5-$- .....E-
0010  00 35 00 00 40 00 39 11 3b 17 8e fa b5 6a c0 a8  -5--@-9- ;....j..
0020  01 14 01 bb da 14 00 21 a8 19 4e 97 d9 e6 d1 10  -.....!-N-----
0030  91 ee 65 0c 8f 7f 2c f4 07 fa 3f 26 3d f3 cf 8c  --e---,--?&=---
0040  d8 02 9c                                     ...
```

Q7:

As you can see below, the source port in 1st packet has become destination port in 2nd packet and the destination port in 1st packet has become source port in 2nd packet also same with Ips.

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows Packet 11, and the bottom screenshot shows Packet 13. Both packets are of type User Datagram Protocol (UDP).

Packet 11:

- Frame 11: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{6C95DF2E-7C0F-4763-8F77-C9A70E9C6508}, id 0
- Ethernet II, Src: IntelCor_eb:35:c5 (08:71:90:eb:35:c5), Dst: zte_de:b8:c8 (24:d3:f2:de:b8:c8)
- Internet Protocol Version 4, Src: 192.168.1.20, Dst: 142.250.181.106
- User Datagram Protocol, Src Port: 55828, Dst Port: 443
- Data (33 bytes)

Packet 13:

- Frame 13: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{6C95DF2E-7C0F-4763-8F77-C9A70E9C6508}, id 0
- Ethernet II, Src: zte_de:b8:c8 (24:d3:f2:de:b8:c8), Dst: IntelCor_eb:35:c5 (08:71:90:eb:35:c5)
- Internet Protocol Version 4, Src: 142.250.181.106, Dst: 192.168.1.20
- User Datagram Protocol, Src Port: 443, Dst Port: 55828
- Data (25 bytes)

The screenshots illustrate a port and IP swap between the two packets. In Packet 11, the source IP is 192.168.1.20 and the source port is 55828. In Packet 13, the source IP is 142.250.181.106 and the source port is 443. The destination IP and port in Packet 13 correspond to the source IP and port of Packet 11.